
# THE CERTIFICATION PRACTICE STATEMENT

# OF

# THE POSTMASTER GENERAL

# As

# A Certification Authority under the Electronic Transactions Ordinance

Date : 31 January 2000

***PREAMBLE***

The Electronic Transactions Ordinance, Cap 553 (the "Ordinance") sets out the legal framework for the e-Cert 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.

The main principle behind cryptography used in electronic transactions is that both parties involved, the sender and receiver use a key which is a set of codes to encrypt (lock) an outgoing message and the receiver must use the same key to decrypt (unlock) the incoming message. To communicate data securely, the sender and receiver must use an effective encryption method.

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

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

HKPost, as a recognized CA, is responsible under the Ordinance for the use of a trustworthy system for the issuance, withdrawal, and publication in a publicly available repository of recognized and accepted digital certificates for secure on-line identification. Such certificates are called "certificates" or "e-Certs". HKPost issues certificates to individual persons ("personal e-Certs"), organisations ("organisational e-Certs") and to organisations that wish to have a certificate issued in a server name owned by that organisation ("server e-Certs").

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 an e-Cert format

Appendix C contains the Master e-Cert Subscriber Agreement

# *1. INTRODUCTION*

## 1.1 Overview

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

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

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.

## 1.2 Community and Applicability

### 1.2.1 Certification Authorities

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

#### 1.2.1.1 Representations by HKPost

By issuing a certificate that refers to this CPS, HKPost represents to Relying Parties who act in accordance with Section 2.1.3 and other relevant sections of this CPS, that HKPost has issued the certificate in accordance with this CPS. By publishing a certificate that refers to this CPS HKPost represents to Relying Parties who act in accordance with Sections 2.1.3 and other relevant sections of this CPS, that HKPost has issued the certificate to the Subscriber identified in it.

#### 1.2.1.2 Effect

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

#### 1.2.1.3 HKPost Right to Subcontract

HKPost may, without consent of any of its subscribers, subcontract its obligations for performing some of the functions required by this CPS provided that the subcontractor agrees to undertake to perform those functions and enters into a contract with HKPost to perform the services.

### 1.2.2 End Entities

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

#### 1.2.2.1 Warranty and Representations by Subscribers

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

a) No person other than the Subscriber 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 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 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 and who have signed a Subscriber Agreement in the appropriate form set out in Appendix C to this CPS. Three classes of e-Cert certificates are issued under this CPS under the Master Subscriber Agreement.

a) **Personal Certificates**

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

b) **Organisational Certificates**

The second class of certificate is issued to organisations that hold a valid business registration certificate issued by the Government of the Hong Kong Special Administrative Region and identifies members or employees of organisations whom the organisation has determined should have a certificate indicating the connection of the member or employee to the organisation. These certificates may be used for the same purposes as Personal Certificates.

c) **Server Certificates**

The third class of certificate is issued to organisations that hold a valid business registration certificate issued by the Government of the Hong Kong Special Administrative Region and that wish to have a certificate issued in a server name owned by that organisation.

### 1.2.4 Certificate Lifespan

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

### 1.2.5 Personal Application at Hong Kong Post Office Premises

All initial applications and applications following the revocation or expiration of an e-Cert will require the applicant personally to attend at a Hong Kong Post Office premise to present the necessary documents of identification, application form and signed subscriber agreements and be prepared to answer any questions concerning the same. In respect of Personal e-Certs this means that all applicants for such e-Certs must attend personally (except the parent or legal guardian of an applicant who is under 18). In respect of Organisational e-Certs, members or employees to be named in the certificate need not attend personally, but the authorised representative of the organisation which is applying for the organisational e-Cert must attend personally. In respect of Server e-Certs this means that the authorised representative of the organisation making the application must attend personally. Upon such personal attendance, the applicants will be required to produce evidence of identity. (See further Section 3 below).

## 1.3 Contact Details

This CPS is administered by:
Hongkong Post
2 Connaught Place, Central
Hong Kong
Attn: Electronic Services Division
Web Site: www.hongkongpost.gov.hk

## *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 at Appendix C to this CPS. 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 Certification Authority Obligations

HKPost is responsible for:

a) Performing CA services and operations, and maintaining the infrastructures related to certificates issued under this CPS, in substantial conformity with the requirements of this CPS
b) Maintaining the security of its private keys

#### 2.1.2 Subscriber Obligations

Subscribers are responsible for:

a) Securely generating a key pair using a trustworthy system during the process for obtaining a certificate

b) Completing the application procedures properly and signing a Subscriber Agreement in the appropriate form as set out in Appendix C and performing the obligations placed upon them by that Agreement

c) Procuring the issuance of a certificate by HKPost including accurately following the directions as to the completion of certificates given in the HKPost e-Cert Customer Kit and accompanying CD Rom.

d) Acknowledging that by accepting the certificate (which will occur during the process for completing the certificate) they are undertaking an obligation to protect the confidentiality (i.e. keep it secret) and the integrity of their private key using reasonable precautions to prevent its loss, disclosure, or unauthorised use

e) 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 HK Post, 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 accepting a certificate they warrant (promise) to HKPost and represent to all Relying Parties that during the operational period of the certificate, the following facts are and will remain true:

   i) No one other than the Subscriber has access to the Subscriber' s private key

   ii) All information and representations made by the Subscriber are true

   iii) The Certificate will be used exclusively for authorised and legal purposes consistent with this CPS.

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

j) Upon becoming so aware of any ground upon which HKPost could revoke the certificate, or upon the Subscriber making a revocation request or upon being notified by HKPost of its intention to revoke the certificate, immediately notifying Relying Parties in any transaction that remains to be completed at the time, that the certificate used in that transaction is liable to be revoked (either by HK Post or at the Subscriber' s request) and stating in clear terms that, as this is the case, the Relying Parties should not rely upon the certificate in respect of the transaction.

#### 2.1.2.1 Subscriber' s Liability

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

### 2.1.3 Relying Party Obligations

Relying Parties relying upon HKPost e-Cert certificates are responsible for:

a) Relying on such certificates only when the reliance is reasonable and in good faith in light of all the circumstances known to the Relying Party at the time of the reliance

b) Before relying upon a certificate determining that the use of the certificate is appropriate for its purposes under this CPS in particular in view of the limited duty of care and limited monetary liability that HKPost undertakes to Relying Parties as set out in this CPS and in the Certificate

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 contract will be uninterrupted or error free or of a higher or different standard than that which should be achieved by the exercise by HKPost, or the officers, employees or agents of Hong Kong Post Office of a reasonable degree and skill and care.**

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

**This means, for example, that provided that the HKPost has exercised a reasonable degree of skill and care, HKPost and Hong Kong Post Office will not be liable for any loss to a Subscriber or Relying Party caused by his reliance upon a false or forged digital signature supported by another Subscriber's recognized certificate issued by HKPost.**

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

### 2.2.2 No Supply of Goods

For the avoidance of doubt, the Subscriber Agreements are not contracts for the supply of goods of any description or at all. Any and all certificates issued pursuant to it remain the property of and in the possession and control of HKPost and no right, title or interest in the certificates is transferred to the Subscriber, who merely has the right to procure the issue of a certificate and to rely upon it and the certificates of other Subscribers in accordance with the terms of the Subscriber Agreements. Accordingly the Subscriber Agreements contain (or is to contain) no express or implied terms or warranties as to the merchantability or fitness of a certificate for a particular purpose or any other terms or conditions appropriate in a contract for the supply of goods. Equally HKPost, in making

available the certificates in a public repository accessible by Relying Parties is not supplying any goods to Relying Parties and likewise gives to Relying Parties no warranty as to the merchantability or fitness for a particular purpose of a certificate nor makes any other representation or warranty as if it were supplying goods to Relying Parties.

### 2.2.3 LIMITATION OF LIABILITY

#### 2.2.3.1 Reasonableness of Limitations

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

#### 2.2.3.2 Limitation on Types of Recoverable Loss

In the event of HKPost's breach of the Subscriber Agreements or of any duty of care, and in particular, of its duty under the Subscriber Agreements to exercise reasonable skill and care and/or duties that may arise to a Subscriber or Relying Party when any certificate issued by HKPost under the PKI is relied upon or used by a Subscriber or Relying Party or anyone else or otherwise howsoever, whether a Subscriber or Relying Party suffers loss and damage as a Subscriber or as a Relying Party as defined by the CPS or otherwise howsoever, **HKPost shall not be liable for any damages or other relief in respect of (1) any direct or indirect: loss of profits or revenue, loss or injury to reputation or goodwill, loss of any opportunity or chance, loss of projects, or the loss or loss of use of any data, equipment or software or (2) for any indirect, consequential or incidental loss or damage even if, in respect of the latter, HKPost has been advised of the likelihood of such loss or damage in advance**.

#### 2.2.3.3 HK$ 1 Million Limit

**Subject to the exceptions that appear below, in the event of HKPost's breach of a Subscriber Agreement or of any duty of care, and in particular, of any duty under the Subscriber Agreements, under this CPS or in law to exercise reasonable skill and care and/or breach of any duties that may arise to a Subscriber or Relying Party when any certificate issued by HKPost under the public 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 $1 million in respect of one certificate**.

#### 2.2.3.4 Time Limit For Making Claims

**Any Subscriber or Relying Party who wishes to make any legal claim upon HKPost arising out of or in any way connected with the issuance, withdrawal or publication of an e-Cert must do so within one year of the date upon which that Subscriber or Relying Party becomes aware of any facts giving rise to the right to make such a claim or (if earlier) within one year of the date when, with the exercise of reasonable diligence, they could have become aware of such facts. For the avoidance of doubt, ignorance of the legal significance of those facts is immaterial. After the expiration of this one year time limit the claim shall be waived and absolutely barred.**

### 2.2.3.5 Hong Kong Post Office Personnel

Neither the Hong Kong Post Office nor any officer or employee or other agent of the Hong Kong Post Office is to be a party to the Subscriber Agreements, and the Subscriber and Relying Parties must acknowledge to HKPost that, as far as the Subscriber and Relying Parties are aware, the Hong Kong Post Office and none of such officers, employees or agents voluntarily accepts or will accept any personal responsibility or duty of care to the Subscriber or Relying Parties in connection with any action or omission done in good faith by any of them in any way connected either with the performance of HKPost of a Subscriber Agreement or any certificate issued by HKPost as a CA and each and every Subscriber and Relying Party accepts and will continue to accept that and undertakes to HKPost not to sue or seek any form of recovery or redress by other legal means whatsoever from any of the foregoing in respect of any act or omission done by that person in good faith (whether done negligently or not) in any way connected with either the performance of HKPost of a Subscriber Agreement or any certificate issued by HKPost as a Certification Authority and acknowledges that HKPost has a sufficient legal and financial interest to protect these individuals from such actions.

### 2.2.3.6 Liability For Wilful Misconduct, Personal Injury or Death

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

### 2.2.3.7 Liability to Consumers

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

### 2.2.3.8 Certificate Notices, Limitations and Reliance Limit

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

> *"The Postmaster General acting by the officers of the Hong Kong Post Office has issued this Certificate as a Certification Authority 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 www.hongkongpost.gov.hk. The law of Hong Kong Special Administrative Region 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 Special Administrative Region.*

*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 certification list prior to reliance;*
*d) Performing all appropriate certificate validation procedures.*

*If, despite the exercise of reasonable skill and care by the Postmaster General and the Hong Kong Post Office, its officers, employees or agents, this certificate is in any way inaccurate or misleading, the Postmaster General, Hong Kong Post Office, its officers, employees or agents, accept no responsibility for any loss or damage to the Relying Parties and the applicable reliance limit that applies to this certificate under the Ordinance in these circumstances is $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 $1 million 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 $1 million and in relation to categories of loss (1) and (2), is HK $0.*

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

*Time Limit For Making Claims*

*Any Relying Party who wishes to make any legal claim upon the Postmaster General arising out of or in any way connected with the issuance, withdrawal or publication of this e-Cert must do so within one year of the date upon which that Relying Party becomes aware of any facts giving rise to the right to make such a claim or (if earlier) within one year of the date when, with the exercise of reasonable diligence, they could have become aware of such facts. For the avoidance of doubt, ignorance of the legal significance of those facts is immaterial. After the expiration of this one year time limit the claim shall be waived and absolutely barred.*

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

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

### 2.2.4 HKPost' s Liability for Accepted but Defective Certificates

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 public key number or digital signature shown on the certificate, no transactions contemplated by the PKI can be completed properly or at all, and that Subscriber' s notifies HKPost of this immediately to permit the certificate to be revoked and (if desired) re-issued, then, if such notification has occurred within 3 months of the acceptance of the certificate and the Subscriber no longer wants a certificate, HKPost, on being satisfied of the existence of any such error will refund the fee. If the Subscriber waits longer than 3 months after acceptance before notifying HKPost of any such error, the fee will not be refunded as of right, but only at the discretion of HKPost.

### 2.2.5 Assignment by Subscriber

Subscribers may not assign their rights under Subscription Agreements or certificates. Any attempted assignment will be void.

### 2.2.6 HKPost' s Ability to Subcontract

HKPost may subcontract the performance of all its obligations under this CPS and Subscriber Agreements without the prior consent or knowledge of Subscribers.

### 2.2.7 Authority to Make Representations

No agent or employee of the Hong Kong Post Office has authority to make any representations on behalf of HKPost as to the meaning or interpretation of this CPS.

### 2.2.8 Variation

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

### 2.2.9 Retention of Title

The physical, copyright, and intellectual rights to all information on the certificate issued under this CPS are and will remain vested in HKPost.

### 2.2.10 Conflict of Provisions

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

### 2.2.11 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.

### 2.2.12 Cross Certification

HKPost reserves the right in all instances to define and determine suitable grounds for cross-certification with another Certification Authority or Postal Certification Authority.

## 2.3 Interpretation and Enforcement (Governing Law)

### 2.3.1 Governing Law

The laws of Hong Kong Special Administrative Region govern this CPS. Subscribers and Relying Parties agree to submit to the non-exclusive jurisdiction of the Courts of Hong Kong Special Administrative Region.

### 2.3.2 Severability, Survival, Merger, and Notice

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

### 2.3.3 Dispute Resolution Procedures

The decisions of HKPost pertaining to matters within the scope of this CPS are final. No alternative dispute resolution procedures regarding Subscriber or Relying Party disputes will be implemented by HKPost.

## 2.4 Fees

Individual e-Certs are available at the cost of HK$150 per certificate per year (although first time subscribers will only be asked to pay HK$50 per certificate);
Organisational e-Certs are available at the cost of HK$150 per certificate per year. However, first time subscribers will only be asked to pay HK$50. An additional administration fee of HK$150 per application (irrespective of the number of subscribers) is payable;
Server e-Certs are available at HK$2,500 per certificate per year.

## 2.5 Publication and Repository

HKPost maintains a repository that contains a list of issued certificates, the current certificate revocation list, the HKPost public key, a copy of this CPS, and other information related to e-Cert certificates which reference this CPS. The repository is available on a substantially 24 hour per day, 7 days per week basis, subject to scheduled maintenance of up to 2 hours per week and any emergency maintenance. HKPost promptly publishes each certificate issued under this CPS in the repository following the processing of an approved e-Cert application.

### 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. These updates are validated through the use of the HKPost private key.

### 2.5.3 Certificate Repository Update Cycle

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

## 2.6 Compliance Audit

Compliance audits conducted on the HKPost's system of issuing, withdrawing and publishing e-Certs to determine if this CPS is being properly followed are performed at least once in every 12 months by professionals with a substantial and documented knowledge of PKI and follow generally accepted accounting practices where applicable.

## 2.7 Confidentiality

The restrictions in this subsection apply to HKPost and any HKPost subcontractors performing

tasks related to HKPost' s system of issuing, withdrawing and publishing e-Certs. Information about Subscribers that is submitted as part of an application for an e-Cert certificate under this CPS will be used only for the purposes collected and is kept confidential except to the extent necessary for HKPost to perform its obligations under this CPS. Such information will not be released without the prior consent of the Subscriber except when required by a court-issued subpoena or order, or when otherwise required by Hong Kong law. HKPost is specifically precluded from releasing lists of Subscribers or Subscriber information (except for compiled data which is not traceable to an individual Subscriber in accordance with Hong Kong law) unless required by a court-issued subpoena or order, or when otherwise required by Hong Kong law.

## *3. IDENTIFICATION AND AUTHENTICATION*

### 3.1 Initial Registration

Save in the case of applicants to be named in organisational e-Certs, each applicant for an e-Cert must appear in person at a designated HKPost premises and present proof of identity as described in sections 3.1.8, 3.1.9, and 3.1.10. In the case of applicants to be named in organisational e-Certs, their attendance is not required, but the authorised representative of the applicant organisation must appear in person.

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

#### 3.1.1 Types of Names

##### 3.1.1.1 Personal e-Certs

Subscribers for Personal e-Certs will be identified in a certificate with a Subscriber Name consisting of:

a) The Subscriber' s name as it appears on the Subscriber' s Hong Kong identity card
b) The Subscriber' s Hong Kong identity card number (the number will be hashed)

##### 3.1.1.1.1 Personal e-Certs issued to Subscriber who are under 18.

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

##### 3.1.1.2 Organisational e-Certs

Subscribers for Organisational e-Certs will be identified in a certificate with a Subscriber Name consisting of:

a) The Subscriber' s name as it appears on the applicant' s Hong Kong identity card/passport

b) The Subscriber organisation' s name as it is registered with the appropriate Hong Kong Government Department or registration agency

c) The organisation' s Hong Kong Company/Business Registration Number.

##### 3.1.1.2.1 The Authorised Representative

Although the authorised representative of the organisation must also become a Subscriber for an organisational e-Cert that person will not be identified in the e-Cert.

##### 3.1.1.3 Server e-Certs

Applicants for Server e-Certs will be identified in a certificate with a Subscriber Name consisting of:

a) The Subscriber organisation's name as it is registered with the appropriate Hong Kong Government Department or registration agency

b) The organisation's Hong Kong Company/Business Registration Number

c) The server name of the server owned by the Subscriber organisation.

#### 3.1.1.3.1 The Authorised Representative

Although the authorised representative of the organisation must also become a Subscriber for a Server e-Cert that person will not be identified in the e-Cert.

### 3.1.2 Need for Names to be Meaningful

All names must be meaningful using commonly understood semantics to determine the identity of the Subscriber.

### 3.1.3 Rules for Interpreting Various Names

The decisions of HKPost in matters concerning name disputes are discretionary, final, and not subject to appeal.

### 3.1.4 Name Uniqueness

Taking all components of the name together, the Subscriber Name shall be unambiguous and unique. However, this CPS does not require that a specific component or element of a name be unique or unambiguous by itself.

### 3.1.5 Name Claim Dispute Resolution Procedure

See section 3.1.3

### 3.1.6 Authentication and Role of Trademarks

Subscribers warrant (promise) to HKPost and represent to Relying Parties that the information supplied by them in the e-Cert application process does not infringe or violate in any way the trademarks, service marks, trade name, company name, or any other intellectual property rights of any third party.

### 3.1.7 Method to Prove Possession of the Private Key

Subscribers must generate their own key pairs and use a trustworthy system for such generation. All Subscribers acknowledge that it is their sole responsibility to maintain the security of the private key related to the public key included in the e-Cert.

### 3.1.8 Authentication of Organisation Identity

When an Organisational e-Cert is applied for, HKPost will follow the procedures outlined in section 3.1.9 except that only the authorised representative must complete the in-person process outlined below and must also become a Subscriber and present (1) either the original, or a copy certified by

the organisation's company chop, of the document containing the resolution of the organisation's board of directors or similar controlling body giving authority to the authorised representative to make the application and identifying the Subscribers to be identified in the organisational e-Cert (2) the Hong Kong identity cards or passports of all Subscribers to be so identified and the authorised representatives own Hong Kong identity card or passport and (3) documentation issued by the appropriate Hong Kong registration agency attesting to the existence of the organisation.

### 3.1.9 Authentication of Individual Identity

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

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

#### 3.1.9.1 Authentication of Individual Identity Where Subscriber Under 18

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

### 3.1.10 Server Certificates

Applications for server e-Certs must be made by the personal attendance at a designated HKPost premises of the Subscriber organisation's authorised representative who must present (1) either the original, or a copy certified by the organisation's company chop, of the document containing the resolution of the organisation's board of directors or similar controlling body giving authority to the authorised representative to make the application and where appropriate proving the ownership of the Domain Name to be identified in the server e-Cert (2) the authorised representative's own Hong Kong identity card or passport and (3) documentation issued by the appropriate Hong Kong registration agency attesting the existence of the organisation.

## 3.2 Certificate Renewal

A certificate renewal request may be authenticated on the basis of a digital signature using the current key pair. Each e-Cert may be renewed once before a new certificate application is required.

### 3.2.1 Personal e-Cert

A Personal e-Cert may be renewed once without going through the process of a face-to-face authentication of the identity of the subscriber which is required when a new certificate application is made. However, upon renewal, the subscriber will be required to generate a new key pair by going

through an electronic interactive process similar to the initial application. A new application form and subscriber agreement will also need to be completed and signed and submitted to HKPost with the appropriate fee.

### 3.2.2 Organisational e-Cert

There is no automatic renewal of an Organisational e-Cert. The process of "Authentication of Organisational identify" as described under Section 3.1.8 will be conducted as if a new application is received.

### 3.2.3 Server e-Cert

There is no automatic renewal of Server e-Cert. The process of "Authentication of Server Certificate" as described under Section 3.1.10 will be conducted as if a new application is received.

## *4. OPERATIONAL REQUIREMENTS*

### 4.1 Certificate Application

Applicants for e-Certs under this CPS must complete and submit an application on a form created by HKPost. All application information transmitted electronically between the applicant and HKPost must use Secure Sockets Layer or a similar protocol prescribed by HKPost from time to time.

### 4.2 Certificate Creation and Issuance

Upon approval of an application, HKPost will prepare the requested certificate and notify the applicant that the certificate is available to be picked up. Acceptance of the certificate by the applicant constitutes the final issuance of the certificate.

### 4.3 The Procedure For Issuing, Checking and Accepting Certificates

a) Hongkng Post will aim to complete the process of an application within the period of time specified in the application form. HKPost will authenticate the identity of each Subscriber and, if and when their identity is authenticated, will notify the Subscriber(s) that the requested certificate is ready to be completed and give details of the electronic interactive process that must followed to ensure completion. This will usually be done by sending to the Subscriber(s) a HKPost e-Cert Customer Kit which will include a CD Rom and PIN mailer (a sealed envelope containing a PIN) and instructions as to how to use them.

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

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

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

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

### 4.4 Certificate Revocation

#### 4.4.1 Circumstances for Revocation

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

Each Subscriber MUST apply to HKPost for the revocation of the certificate in accordance with the revocation procedures in this CPS whenever 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.

HKPost may revoke a certificate 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 a Subscriber Agreement;
e) Is required to do so by any regulation, or law applicable to the certificate;
f) Knows or has reasonable cause to believe that the Subscriber whose details appear on the certificate or the authorised representative:

   (i) Is dead or has died;

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

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

   and where a Subscriber is an Organisation that :

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

   ii) The Subscriber has entered into a composition or a scheme of arrangement or a voluntary arrangement within the meaning of the Bankruptcy Ordinance (Cap.6) within 5 years preceding the date of intended revocation;

   iii) A director, officer or employee of the Subscriber has been convicted of an offence for which it was necessary to find that that person acted fraudulently, corruptly or dishonestly or an offence under the Electronic Transactions Ordinance;

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

### 4.4. 2 Revocation Request Procedure

Based on a request by fax, HKPost will place a "hold" on the Certificate which effectively suspends, but does not revoke the Certificate. The Subscriber then has to send his or her or its original Letter of Revocation to HKPost to complete the revocation process. In-person or digitally signed requests will be processed directly as immediate revocation without the "hold" procedure. HKPost will endeavour to issue a Notice of Revoation to such subscribers within one week following the request for revocation.

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 | Excluded |

For any weekday (Monday -Saturday) on which 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.

### 4.4.3 Service Pledge & Certificate Revocation List Update

a) HKPost will exercise reasonable endeavours to see that within 2 working days of (1) HKPost receiving a revocation request from the Subscriber or (2) In the absence of such a request, the decision by HKPost to suspend or revoke the certificate, the suspension or revocation is posted to the Certification 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. [Certification 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 cycle and rainstorm warning signal is hoisted, are not working days.

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

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

Parties who receive such a notification from Subscribers

but who complete the transaction despite such notification. HKPost shall be under no liability to Relying Parties in respect of the period between HKPost' s decision to suspend or revoke a certificate (either in response to a request or otherwise) and the appearance of this information on the Certification 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.

### 4.4.4 Effect of Revocation

Revocation terminates a certificate as of the time that HKPost processes the revocation action and posts it to the CA database.

## 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:

- Installation and modification of CA equipment
- All instances of certificate issuance
- All instances of certificate revocation
- Changes of HKPost employee access rights that affect the certificate creation, issuance, or revocation processes
- Internal HKPost key pair generation pertinent to this PKI

### 4.5.2 Frequency of Processing Log

Temporary audit log files are archived and digitally signed by HKPost on a daily basis.

### 4.5.3 Retention Period for Audit Logs

Archived audit log files are retained for 7 years.

### 4.5.4 Protection of Audit Logs

Audit logs are afforded protection similar to that afforded other critical files within the HKPost CA operation.

### 4.5.5 Audit Log Backup Procedures

The backup procedures for audit logs follow requirements and procedures similar to those afforded other critical files within the HKPost CA system.

### 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

The following data and files are archived by (or on behalf of) HKPost:

- Computer security audit data
- Certificate application data
- Certificates issued
- Certificate revocation lists generated
- Material correspondence between HKPost and Subscribers

### 4.6.2 Archive Retention Period

Key and certificate information is securely maintained for 7 years. Audit trail files are maintained online as deemed appropriate by HKPost.

### 4.6.3 Archive Protection

Archived media maintained by HKPost is protected from unauthorised access by various physical and cryptographic means. Protective measures are used to protect the archiving media from environmental threats such as temperature, humidity, and magnetism.

### 4.6.4 Archive Backup Procedures

Backup copies of the archives are created and maintained in case of the loss or destruction of the primary archives.

### 4.6.5 Timestamping

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

## 4.7 Key Changeover

The lifespan of the HKPost e-Cert root key will be 10 years from January 2000 and public announcement will be made prior to key changeover.

## 4.8 Disaster Recovery and Key Compromise Plans

### 4.8.1 Disaster Recovery Plan

HKPost has a disaster recovery/business resumption plan in place for providing CA services in accordance with this CPS should the primary operations site be rendered nonfunctional.

### 4.8.2 Key Compromise Plan

HKPost will promptly notify Subscribers if a private key relevant to 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, replacement certificates.

## 4.9 Certification Authority Termination

In the event that HKPost ceases to operate as a CA, Subscribers will be promptly notified of the termination. Certificates issued by HKPost that reference this CPS will be posted in a recognized repository until the expiry of the certificates.

## *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 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

See sections 4.6.3, 4.6.4, and 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 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.

## 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 their employees and of the satisfactory performance of the employees' 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*

### 6.1 Key Pair Generation and Installation

#### 6.1.1 Key Pair Generation

Key pairs for HKPost and Subscribers are generated through a procedure such that the private key cannot be accessed by anyone other than the authorised user of the key pair unless there is some compromise of the procedure by the authorised user.

#### 6.1.2 Subscriber Public Key Delivery

The Subscriber' s public key must be transferred to HKPost using a method designed to ensure that:

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

#### 6.1.3 Public Key Delivery to Subscriber

The public key of each HKPost key pair used for the CA' s digital signatures is available on-line. 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 cryptomodule.

#### 6.1.6 Key Usage Purposes

Keys used in HKPost e-Cert may be used for either digital signature or non-repudiation services. The HKPost signing 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

Subscriber private keys must be created in a cryptomodule validated to at least FIPS 140-1 Level 1.

#### 6.2.2 Private Key Single-Person Control

All Subscribers must maintain a one-person private key environment. No private key may be shared between two or more individuals.

#### 6.2.3 Private Key Escrow

No over-all key escrow process is planned for private keys in the e-Cert system used by HKPost. Applicants for a HKPost e-Cert who desire key escrow services should contact the Hongkong Post Electronic Services Division at 2927 7132 for further details and arrangements.

### 6.2.4 Backup of HKPost Private Keys

Backup of the HKPost private key is performed in a manner that requires more than one person to activate the backup private key. No other keys are backed-up.

## 6.3 Other Aspects of Key Pair Management

A HKPost public key will be used for no more than 10 years. All HKPost key generation, key storage, and certificate and revocation list signing operations are performed in a hardware cryptographic module.

## 6.4 Computer Security Controls

### 6.4.1 Individual Accountability

Each user of the e-Cert PKI is identified individually with no sharing of identifiers or use of group identifiers. Only the Subscriber named in an e-Cert may use it. The Subscriber for a Server e-Cert may use the certificate only in respect of one server.

### 6.4.2 Computer Security Rating

**The HKPost e-Cert PKI computer centre is compliant with rating BS7799.**

### 6.4.3 Computer Security Training

HKPost employees working with the e-Cert PKI are trained in commercially reasonable computer security practices and procedures.

## 6.5 Life Cycle Technical Security Controls

### 6.5.1 Security Management Controls

HKPost systems used in the creation or issuance of certificates are tested at least every twelve months in an effort to prevent hacking or other unauthorised access.

## 6.6 Network Security Controls

The HKPost server and CA database are protected by firewalls configured to allow only the protocols and commands required for the CA services set forth in this CPS.

## 6.7 Cryptographic Module Engineering Controls

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

## *7. CERTIFICATE AND CERTIFICATION 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.

### 7.2 Certificate Revocation List Profile

The HKPost certificate revocation list is in the X.509 version 2 format.

## *8. CPS ADMINISTRATION*

### 8.1 CPS Change Procedures

All changes to this CPS must be approved and published by HKPost. The CPS changes will be effective upon publication by HKPost in the repository and are binding on all applicants for new certificates and upon all holders of existing certificates as those certificates are renewed.

### 8.2 Publication and Notification Procedures

A copy of this CPS is available on the Internet at www.hongkongpost.gov.hk/pki and in the HKPost repository. A paper copy of this CPS or other related documents may be requested at the following address:

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

Changes to this CPS are available at the same locations.

***APPENDIX A***
**Glossary**

***APPENDIX B***
**e-Cert Format**

***APPENDIX C***
**Master e-Cert Subscriber Agreement**

*APPENDIX A*

## A.1 Glossary

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

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

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

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

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

**"Asymmetric Cryptosystem"** means a system capable of generating a secure key pair, consisting of a private key for generating a digital signature and a public key to verify the digital signature.

**Certificate or "e-Cert"** means a record which:-

a) is issued by a certification authority for the purpose of supporting a digital signature which purports to confirm the identity or other significant characteristics of the person who holds a particular key pair;
b) identifies the certification authority issuing it;
c) names or identifies the person to whom it is issued;
d) contains the public key of the person to whom it is issued; and
e) is signed by a responsible officer of the certification authority issuing it.

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

**"Certification Practice Statement"** means a statement issued by a certification authority to specify the practices and standards that the certification authority employs in issuing certificates

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

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

**"Digital Signature"**, in relation to an electronic record, means an electronic signature of the signer generated by the transformation of the electronic record using an asymmetric cryptosystem

and a hash function such that a person having the initial untransformed electronic record and the signer's public key can determine:-

(a) whether the transformation was generated using the private key that corresponds to the signer's public key; and

(b) whether the initial electronic record has been altered since the transformation was generated.

**"Electronic Record"** means a record generated in digital form by an information system, which can be

(a) transmitted within an information system or from one information system to another; and

(b) stored in an information system or other medium.

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

**"Information"** includes data, text, images, sound, computer programmes, software and databases.

**"Information System"** means a system which –

(a) processes information;

(b) records information;

(c) can be used to cause information to be recorded, stored or otherwise processed in other information systems (wherever situated); and

(d) can be used to retrieve information, whether the information is recorded or stored in the system itself or in other information systems (wherever situated).

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

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

**"Key Pair"**, in an asymmetric cryptosystem, key pair means a private key and its mathematically related public key, where the public key can verify a digital signature that the private key generates.

**"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 Transaction Ordinance; or

(c) a certificate designated as a recognized certificate issued by the certification authority referred to in section 34 of Electronic Transactions Ordinance.

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

**"Record"** means information that is inscribed on, stored in or otherwise fixed on a tangible medium or that is stored in an electronic or other medium and is retrievable in a perceivable form.

**"Reliance Limit"** means the monetary limit specified for reliance on a recognized certificate.

**"Repository"** means an information system for storing and retrieving certificates and other information relevant to certificates.

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

**"Rule of law"** means

(a) an Ordinance;

(b) a rule of common law or a rule of equity; or

(c) customary law.

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

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

**"Subscriber"** means a person (who may be a certification authority) who has signed a Subscriber Agreement and who-

(a) is named or identified in a certificate as the person to whom the certificate is issued;

(b) has accepted that certificate; and

(c) holds a private key which corresponds to a public key listed in that certificate.

**"Trustworthy System"** means computer hardware, software and procedures that—

(a) are reasonably secure from intrusion and misuse;

(b) are at a reasonable level in respect of availability, reliability and ensuring a correct mode of operations for a reasonable period of time;

(c) are reasonably suitable for performing their intended function; and

(d) adhere to generally accepted security principles.

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

(a) the digital signature was generated using the private key corresponding to the public key listed in a certificate; and

(b) the electronic record has not been altered since its digital signature was generated,

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

For the purpose of the Electronic Transactions Ordinance, a digital signature is taken to be supported by a certificate if the digital signature is verifiable with reference to the public key listed in a certificate the subscriber of which is the signer.

**Appendix B**

## Hongkong Post e-Cert Format

| | | e-Cert (Personal) | e-Cert (Personal/Minor) | e-Cert (Organisational) | e-Cert (Server) |
|---|---|---|---|---|---|
| **Standard Fields** | | | | | |
| **Version** | | V3 | V3 | V3 | V3 |
| **Serial Number** | | [generated] | [generated] | [generated] | [generated] |
| **Signature Algorithm ID** | | sha1RSA | sha1RSA | sha1RSA | sha1RSA |
| **Issuer Name** | | cn=Hongkong Post e-Cert CA,<br>o=Hongkong Post,<br>c=HK | cn=Hongkong Post e-Cert CA,<br>o=Hongkong Post,<br>c=HK | cn=Hongkong Post e-Cert CA,<br>o=Hongkong Post,<br>c=HK | cn=Hongkong Post e-Cert CA,<br>o=Hongkong Post,<br>c=HK |
| **Validity** | **Not Before** | [UTC Time] | [UTC Time] | [UTC Time] | [UTC Time] |
| | **Not After** | [UTC Time] | [UTC Time] | [UTC Time] | [UTC Time] |
| **Subject Name** | | cn=[HKID name][1],<br>ea=[email address],<br>ou=[SRN][2],<br>o=Hongkong Post e-Cert (Personal),<br>c=HK | cn=[HKID name][1],<br>ea=[email address],<br>ou=[SRN][2],<br>o=Hongkong Post e-Cert (Personal/Minor),<br>c=HK | cn=[name],<br>ea=[email address],<br>ou=[SRN][2],<br>ou=[BRN+CI/CR+Others][4],<br>ou=[Organization],<br>ou=[Organization branch/dept],<br>o=Hongkong Post e-Cert (Organisational),<br>c=HK | cn=[URL],<br>ou=[SRN][2],<br>ou=[BRN+CI/CR+Others][4],<br>ou=[Organization],<br>ou=[Organization branch/dept],<br>o=Hongkong Post e-Cert (Server),<br>c=HK |
| **Subject Public key Info** | **Algorithm ID** | RSA | RSA | RSA | RSA |
| | **Public Key** | [generated and supplied from subscriber's browser during certificate request ][3] | [generated and supplied from subscriber's browser during certificate request ][3] | [generated and supplied from subscriber's browser during certificate request ][3] | [generated and supplied from subscriber's CSR ] |
| **Issuer Unique Identifier** | | Not used | Not used | Not used | Not used |
| **Subject unique identifier** | | Not used | Not used | Not used | Not used |
| **Standard Extensions** | | | | | |
| **Authority Key Identifier** | **Issuer** | cn=Hongkong Post Root CA,<br>o=Hongkong Post,<br>c=HK | cn=Hongkong Post Root CA,<br>o=Hongkong Post,<br>c=HK | cn=Hongkong Post Root CA,<br>o=Hongkong Post,<br>c=HK | cn=Hongkong Post Root CA,<br>o=Hongkong Post,<br>c=HK |
| | **Serial Number** | [Inherited from issuer] | [Inherited from issuer] | [Inherited from issuer] | [Inherited from issuer] |
| **Basic Contraints** | **Subject Type** | End Entity | End Entity | End Entity | End Entity |
| | **Path Length Contraint** | None | None | None | None |
| **Key Usage** | | Digital Signature, Key Encipherment | Digital Signature, Key Encipherment | Digital Signature, Key Encipherment | Key Encipherment |
| **Subject Alternative Name** | **DNSName** | [protect(HKID)][5] | [protect(HKID)][5] | Not used | Not used |
| | **rfc822** | [email address] | [email address] | [email address] | Not used |
| **NstScape Extensions** | | | | | |
| **Netscape Cert Type** | | SSL client, S/MIME | SSL client, S/MIME | SSL client, S/MIME | SSL server |
| **Netscape SSL Server Name** | | Not used | Not used | Not used | [URL] |
| **Netscape Comment** | | Hongkong Post e-Cert | Hongkong Post e-Cert | Hongkong Post e-Cert | Hongkong Post e-Cert |

**Notes:**

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

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

[3] 1024-bits

[4] Business Registration Number (BRN): 16 digits, Certificate of Incorporation (CI)/ Certificate of Registration (CR): 8 digits, Others: max. 30 characters (blank if null).

[4] For HKSAR government departments, BRN and CI/CR are all zeroes, department name in abbreviation (e.g. HKP for Hongkong Post) is placed in Others.

[5] sha1[sha1RSA[HKID]], HKID includes the check digit but without parenthesis.

**Appendix C**

# SUBSCRIBER AGREEMENT

IMPORTANT: READ CAREFULLY

THIS SUBSCRIBER AGREEMENT IS ENTERED INTO BY YOU THE SUBSCRIBER(S) AND THE POSTMASTER GENERAL AS REPRESENTED BY THE HONG KONG POST OFFICE. BEFORE SUBMITTING THE DIGITAL CERTIFICATE APPLICATION, YOU MUST FIRST READ AND ACCEPT THE TERMS OF THIS AGREEMENT BY SIGNING AND DATING THIS AGREEMENT IN THE SPACES PROVIDED AT THE END OF THIS AGREEMENT. IF YOU DO NOT ACCEPT THE TERMS OF THIS AGREEMENT, THE CERTIFICATE APPLICATION WILL NOT BE ACCEPTED AND A CERTIFICATE WILL NOT BE ISSUED.

---

In consideration for the payment of the fees charged for the issue of the certificate and of the terms and conditions set out below, the Postmaster General as represented by the Hong Kong Post Office (HKPost) and you the subscriber(s), intending to be legally bound, agree as follows:

**HKPost**

1. The Postmaster General is a recognised Certification Authority for the purposes of the Electronic Transactions Ordinance, Cap. 553 ("the Ordinance") . Under the Ordinance the Postmaster General may perform the functions and provide the services of a certification authority by the officers of the Hong Kong Post Office. Accordingly, the Postmaster General, for the purposes of this agreement, is represented by the Hong Kong Post Office, and is identified herein as **HKPost** .
   HKPost has published for public knowledge a Certification Practice Statement ("CPS") for each type, class or description of recognised certificates that it issues as a Certification Authority. This contract sets out the terms upon which HK Post will issue an e-Cert Certificate ("certificate") in conformity with the CPS.

**Subscribers.**

2. **Subscribers.** Subscribers are individuals and Organisations who procure the creation and issuance of a certificate in return for their agreement to be bound by all the terms and conditions of this agreement and who have signed it by themselves or by their authorised representatives. **If there is more than one Subscriber to this agreement, each Subscriber agrees to be liable to HK Post for the performance of this agreement by each of the other Subscribers as well as for the Subscriber' s own performance of it.**

   **Personal e-Cert Subscribers.** If you are applying for a Personal e-Cert and are the person whose details are to appear upon the Certificate, then you may become a Subscriber and a

certificate will be issued if you agree to and sign this agreement.

**Personal e-Cert Subscribers who are Minors.** If you are under 18 and are applying for a personal certificate, you can become a Subscriber and a certificate will be issued with your details on it, but ONLY if BOTH you and one of your parents (or your legal guardian) agree to be Subscribers and your parent or legal guardian agrees (by signing this agreement) to undertake and perform the obligations of a Subscriber in relation to your certificate as if it were a certificate issued in the name of the parent or guardian **and the parent or legal guardian also undertakes to be liable to HKPost if you do not comply with the terms and conditions of this agreement and this causes loss or damage to HKPost**, but the parent or legal guardian will not (unless they make a separate application) have a certificate issued in their name. Further, the certificate that is issued in the name of a minor may carry a special warning to relying parties, as under the law, minors might not be bound by certain contracts.

**Organisational e-Cert Subscribers.** If you are applying for an Organisational e-Cert, and it is intended that your details will appear on the certificate, a certificate will be issued ONLY if (i) you are (and hereby warrant that you are) a member or employee of the organisation concerned and you are authorised by the organisation to hold and use the certificate and you become a Subscriber AND (ii) the Organisation concerned, by the authorised representative referred to in the application form, also signs and impresses the Organisation's chop upon this agreement and **BOTH the Organisation and the Authorised Representative thereby become Subscribers and agree to undertake and perform all the terms of this agreement and all the obligations of a Subscriber in relation to the certificate.**

**Server e-Cert Subscribers**. If you are the authorised representative referred to in the application form and are applying on behalf of an Organisation for an e-Cert to be issued in a Server Name owned by that Organisation, a certificate will be issued ONLY if the Organisation concerned, through you, signs and impresses the Organisation's chop upon this agreement and **BOTH you and the Organisation thereby become Subscribers and agree to undertake and perform all the obligations of a Subscriber in relation to the certificate.**

**Relying Parties**

3. **Relying Parties.** Under the CPS there are two types of end entities: Subscribers (as defined therein) and Relying Parties. Subscribers are defined therein as individuals or organisations who have procured the issuance of a certificate. Relying parties are defined therein as entities that have accepted a certificate for use in a transaction. The present agreement is intended to govern the relationship between HKPost and Subscribers (as defined in clause 2 above) in their capacity both as Subscribers and Relying Parties as defined in the CPS. **This may well mean (and it is the intention of this agreement) that your rights against HKPost as a Relying Party may be limited under this agreement in a way that they would not be if you were not a Subscriber bound by its terms**. If you do not accept this, then do not sign the agreement.

**Recognition and Incorporation of Certification Practice Statement (CPS)**

4. **The CPS is a VERY IMPORTANT DOCUMENT because it is intended to incorporate the entirety of the CPS into this agreement, with each Subscriber undertaking to HKPost all the obligations of Subscribers and Relying Parties set out in the CPS**. **The CPS also contains IMPORTANT LIMITATIONS AND EXCLUSIONS** on HKPost's liability to you (including ones which relate to negligence) which are intended to become binding upon you if you enter into this agreement. The CPS is available on the HKPost's web site at www.hongkongpost.gov.hk or at any Hong Kong Post Office and **you and each subscriber can and should read the CPS before entering into this agreement**. By accepting the terms of this agreement, you ACKNOWLEDGE that you and each Subscriber under this agreement has had **FULL AND COMPLETE NOTICE of the obligations upon Subscribers and Relying Parties set out in the CPS and of the limitation and exclusion clauses set out therein (including those relating to negligence)**. You further agree to be bound by the provisions in the CPS applicable to you the Subscriber, both as a Subscriber and Relying Party as described in the CPS, all the terms and conditions of which, including those **limiting and excluding HKPost's liability**, are hereby incorporated into this agreement as if set out word for word herein. Some but not all of the obligations of you the Subscriber and of HKPost are set out below for your convenience. IF YOU DO NOT UNDERSTAND THE CPS, YOU SHOULD NOT SIGN THIS AGREEMENT AND SHOULD NOT PARTICIPATE IN THE PUBLIC KEY INFRASTRUCTURE INITIATIVE.

**Subscriber Acknowledgement of Understanding of the CPS.**

5. By accepting the terms of this agreement, you acknowledge:
   - an awareness of the operation of a public key infrastructure system
   - an understanding of the limits of such a system
   - an understanding of the necessity of maintaining the security of the private key related to the public key named in your digital certificate.

**The Procedure For Issuing, Checking and Accepting Certificates.**

6. (1) HKPost will aim to complete the process of an application within the period of time specified in the application form. HKPost will authenticate the identity of each Subscriber and, if and when their identity is authenticated, will notify the Subscriber(s) that the requested certificate is ready to be completed and give details of the electronic interactive process that must followed to ensure completion. This will usually be done by sending to the Subscriber(s) a HKPost e-Cert Customer Kit which will include a CD Rom and PIN mailer (a sealed envelope containing a PIN) and instructions as to how to use them.

   (2) When following the interactive procedures for the completion of the certificate, you

will be given the opportunity to **CHECK** to see that **all the information and each representation made by the Subscriber(s) included in the certificate is accurate and true**. Each Subscriber hereby promises to HKPost that this check will be done and done properly.

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

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

**Consequences of Acceptance**

7. By accepting a certificate issued under the CPS, each Subscriber warrants (promises) to HKPost and represents to all other relevant parties (including any Relying Parties) that during the operational period of the certificate the following facts are and will remain true:

- No other person than the Subscriber has had access to the Subscriber's private key;
- Each digital signature generated using the Subscriber's private key which corresponds to the public key contained in the Subscriber's certificate, is the digital signature of the Subscriber;
- All information and representations made by the Subscriber included in the certificate are true;
- The certificate will be used exclusively for authorised and legal purposes consistent with the CPS;
- 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 intellectual property rights of any third party.

8. By accepting the certificate each Subscriber undertakes an obligation to keep the Subscriber's private key secret and to protect its confidentiality and integrity by using reasonable precautions to prevent its loss, disclosure, or unauthorised use. This will include treating any password or other access control device related to use of the private key as confidential information and not disclosing any access control device to anyone else.

9. **Subscriber's Liability**. Each Subscriber acknowledges that if the above warranty to HKPost is broken, or the representations set above are or become false, or the obligation referred to above is broken, each Subscriber is or may become liable under this contract and/or in law to pay HKPost and/or, under the law, other persons damages in respect of liabilities or loss and damage they may incur or suffer in consequence.

10. **HKPost's Liability for Accepted but Defective Certificates**. If, after acceptance of the certificate, you find that because of any error in the public key number or digital signature

shown on the certificate, no transactions contemplated by the public key initiative can be completed properly or at all, then you must notify HKPost of this immediately to permit the certificate to be revoked and (if desired) re-issued or, if such notification has occurred within 3 months of the acceptance of the certificate and you no longer want a certificate, to permit HKPost (on being satisfied of the existence of any such error) to refund the fee. If you wait longer than 3 months after acceptance before notifying HKPost of any such error, the fee will not be refunded as of right, but only at the discretion of HKPost.

**Reporting**

11. **Reporting changes in information on Certificate.** Each Subscriber agrees to notify HKPost of any change in the information in the certificate provided by the Subscriber IMMEDIATELY on each occasion of becoming aware of any such change during the period in which the Subscriber's certificate is valid and HKPost will suspend or revoke the certificate upon such notification in accordance with the CPS procedures.

**Reporting Loss or Compromise of Private Key.** Each Subscriber agrees to report to HKPost any loss or compromise of the Subscriber's 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) and HKPost will suspend or revoke the certificate upon such notification in accordance with the CPS procedures.

**Reporting Grounds For Revocation**. The further grounds upon which HKPost may revoke a certificate are set out below. Each subscriber (or in the case of death, his personal representatives or other persons responsible in law for the affairs of the deceased subscriber) shall notify HKPost IMMEDIATELY of any fact which may give rise to HKPost, upon such further grounds, having the right to revoke the certificate for which the Subscriber is responsible under this contract.

12. **Subscriber's Liability for not Reporting.** If the reporting obligations set out above are not complied with properly or at all, then:
    - HKPost accept's no liability for any consequences, especially not for any loss or damage that may result to the Subscriber or anyone else;
    - each Subscriber is or may become liable to pay HKPost (and possibly, under the law, other persons) damages in respect of liabilities incurred or loss and damage suffered in consequence.

**Duration**

13. **Limitation of Time**. Certificates issued under this agreement are valid for one year.

**Obligations of Subscriber as a Relying Party**

14. Each Subscriber agrees that, when they use the public key infrastructure system and become Relying Parties, they are solely responsible (as between themselves and HKPost) for:
    - Relying on certificates 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;
    - Before accepting a certificate determining that the use of the certificate is appropriate for its purposes under the CPS;
    - Checking the status of the certificate on the certification revocation list prior to reliance upon it;
    - Performing all appropriate certificate path validation procedures.

**Revocation**

15. Each Subscriber may revoke the certificate for which they are responsible under this contract at any time for any reason by following the revocation procedures set out in the CPS.

16. HKPost may revoke a certificate in accordance with the procedures in the CPS whenever it:

    1. Knows or reasonably suspects that a Subscriber's private key has been compromised;
    2. Knows or reasonably suspects that any details upon a certificate are not true or have become untrue or that the certificate is otherwise unreliable;
    3. Determines that a certificate was not properly issued in accordance with the CPS;
    4. Determines that the Subscriber had failed to meet any of the obligations set out herein;
    5. Is required to do so by any regulation, or law applicable to the certificate;
    6. Knows or has reasonable cause to believe that the Subscriber whose details appear on the certificate or the authorised representative:
        (i) Is dead or has died;
        (ii) Is or has become an undischarged bankrupt or has entered into a composition or scheme of arrangement or a voluntary arrangement within the meaning of the Bankruptcy Ordinance (Cap. 6) within 5 years preceding the date of revocation;
        (iii) Has been convicted in Hong Kong or elsewhere of an offence for which it was necessary to find that the person acted fraudulently, corruptly or dishonestly or an offence under the Electronic Transactions Ordinance.

    and where a Subscriber is an Organisation that :

        (i) the Subscriber is in liquidation, or a winding up order relating to the Subscriber has been made by any Court of competent jurisdiction;
        (ii) The Subscriber has entered into a composition or a scheme of arrangement or a voluntary arrangement within the meaning of the

Bankruptcy Ordinance (Cap.6) within 5 years preceding the date of intended revocation;

(iii) A director, officer or employee of the Subscriber has been convicted of an offence for which it was necessary to find that that person acted fraudulently, corruptly or dishonestly or an offence under the Electronic Transactions Ordinance;

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

**Obligations of HKPost**

17. HKPost hereby agrees with each Subscriber to exercise a reasonable degree of skill and care in performing the obligations and exercising the rights it has as a Certification Authority set out herein and in the CPS.**HKPost does not undertake any absolute obligations to the Subscriber(s). It does not warrant that the services it provides under this contract will be uninterrupted or error free or of a higher or different standard than that which should be achieved by the exercise by HKPost, its servants or agent of reasonable degree of skill and care in carrying out this contract.**

**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 the CPS, suffers any liability, loss or damage of whatsoever nature arising out of or in connection with the public key infrastructure system as described in the CPS, including loss and damage consequent upon reasonable reliance upon a certificate of another Subscriber, each Subscriber agrees that HKPost is 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 will not be liable for any loss to a Subscriber caused by his reliance upon a false or forged digital signature supported by another Subscriber' s recognised certificate issued by HKPost.**

**This means, also, that, provided HKPost has exercised a reasonable degree of skill and care to avoid and/or mitigate the effects of matters beyond its control, HKPost is not liable for the adverse effects to Subscribers 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.

18. For the avoidance of doubt, this is not a contract for the supply of goods of any description or at all. Any and all certificates issued pursuant to it remain the property of and in the possession and control of HKPost and no right, title or interest in the certificates is transferred to the Subscriber, who merely has the right to procure the issue of a certificate

and to rely upon it and the certificates of other Subscribers in accordance with the terms of this contract. Accordingly this contract contains (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.

**LIMITATION OF LIABILITY**

19. Each Subscriber acknowledges that the public key infrastructure initiative and HKPost' s role as a Certification Authority within that initiative are new and innovative ventures, in which the sum received by HKPost from the Subscriber is modest compared to the burden that could be placed upon HKPost if HKPost were liable without limit for damages under or in connection with this contract or the issue by HKPost of certificates under the public key infrastructure initiative. Accordingly, each Subscriber agrees that it is reasonable for HKPost to limit its liabilities as set out in this contract and in the CPS.

20. In the event of HKPost' s breach of this contract or of any duty of care, and in particular, of its duty under this contract to exercise reasonable skill and care and/or duties that may arise to a Subscriber when any certificate issued by HKPost under the public key infrastructure initiative is relied upon or used by that Subscriber or anyone else or otherwise howsoever, whether a Subscriber suffers loss and damage as a Subscriber or as a Relying Party as defined by the CPS or otherwise howsoever, **HKPost shall not be liable for any damages or other relief in respect of (1) any direct or indirect: loss of profits or revenue, loss or injury to reputation or goodwill, loss of any opportunity or chance, loss of projects, or the loss or loss of use of any data, equipment or software or (2) for any indirect, consequential or incidental loss or damage even if, in respect of the latter, HKPost has been advised of the likelihood of such loss or damage in advance**.

21. Subject to the exceptions that appear below, in the event of HKPost' s breach of this contract or of any duty of care, and in particular, of its duty under this contract to exercise reasonable skill and care and/or duties that may arise to a Subscriber when any certificate issued by HKPost under the public key infrastructure initiative is relied upon or used by that Subscriber or anyone else or otherwise howsoever, whether a Subscriber 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, 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 $1 million in respect to one certificate**.

.

22. **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 a party to this agreement, and the Subscriber acknowledges to HKPost that, as far as the Subscriber is aware, the Hong Kong Post Office and none of its officers, employees or agents voluntarily accepts or will accept

any responsibility or duty of care to the Subscriber 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 this agreement or any certificate issued by HKPost as a Certification Authority and each and every Subscriber 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 this agreement or any certificate issued by HKPost as a Certification Authority and acknowledges that HKPost has a sufficient legal and financial interest to protect the Hong Kong Post Office and these individuals from such actions.

23. **Time Limit For Making Claims.** Any Subscriber who wishes either as a Subscriber or Relying Party to make any legal claim upon HKPost, arising out of or in any way connected with the issuance, withdrawal or publication of any e-Cert must do so within one year of the date upon which that Subscriber 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.

24. **Fraud or 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 of this contract and is not limited or excluded by any such provision.

25. **Consumers.** If you are a Subscriber who has not made this contract in the course of a business or held yourself out as doing so, it is possible that, as a matter of law, some or all of the limitations of liability that apply in the event of HKPost' s failure to carry out this contract with reasonable skill and care do not apply to any claim you may have.

## MISCELLANEOUS PROVISIONS

### Assignment by Subscribers

26. Neither this agreement nor your digital certificate may be assigned by you. Any attempted assignment will be void.

### HKPost' s Ability to Subcontract

27. You allow HKPost to subcontract the performance of all its obligations under this agreement.

**Severability**

28. If any terms, or any part of any terms, of this contract are found by any court to be illegal, void or unenforceable they shall be severed and deleted, but this shall not affect the validity and enforceability of the remaining terms, or remaining part of any terms, of this contract.

**Governing Law**

29. This agreement is governed by the laws of Hong Kong Special Administrative Region (SAR). The parties agree to submit any disputes arising out of, relating to or in any way connected with this agreement (by any common facts or parties or otherwise howsoever) to the non-exclusive jurisdiction of the Courts of Hong Kong SAR.

**Entire Agreement**

30. This agreement, including the incorporated CPS, constitutes the entire agreement between the parties and supersedes all prior or contemporaneous agreements or understanding between the parties regarding the issuance of digital certificates.

**Fiduciary Relationships**

31. HKPost is not an agent, fiduciary, trustee or other representative of the Subscriber or Relying Parties. Subscribers have no authority to bind HKPost by contract or otherwise to any obligation.

**Authority to make representations**

32. 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 contract.

**Variation**

33. HKPost has the right to propose variations or additions to this agreement, and shall do so by giving you notice in writing of such proposed changes and notice of the methods by which you may accept them.

34. An employee of the Hong Kong Post Office may only vary this agreement with the written authority of the Postmaster General.

**Retention of title**

35. The physical, copyright, and intellectual rights to all information on the certificate issued under this contract are and will remain vested in HKPost.

**Interpretation**

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

IF YOU AGREE TO THE TERMS OF THIS AGREEMENT, SIGN AND DATE THIS AGREEMENT IN THE SPACES PROVIDED BELOW.

IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT SIGN IT.

THE SIGNING OF THIS AGREEMENT AND ITS RECEIPT BY HKPOST WILL NOT GUARANTEE THAT YOUR APPLICATION FORM WILL BE ACCEPTED. IF IT IS REJECTED, YOU WILL BE NOTIFIED. IF YOUR APPLICATION FORM IS ACCEPTED YOU WILL BE BOUND BY THE TERMS HEREIN AS WELL AS THOSE SET OUT IN THE CPS.