THE CERTIFICATION PRACTICE STATEMENT

OF

THE POSTMASTER GENERAL

As

A Recognized Certification Authority
under the Electronic Transactions Ordinance

for

Hongkong Post e-Cert (Personal)
Hongkong Post e-Cert (Organisational)
Hongkong Post e-Cert (Encipherment)
Hongkong Post e-Cert (Server)

Date : 1 December 2017
OID : 1.3.6.1.4.1.16030.1.1.36

Table of Contents

PREAMBLE

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

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

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

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

Since 1 April 2007, HKPost CA operations have been outsourced with private sector participation. Currently, HKPost has awarded a contract ("Contract") to Certizen Limited for operating and maintaining the systems and services of the HKPost CA as stipulated in this CPS from 1 April 2012 to 31 March 2018.

Under the Contract, Certizen Limited, after obtaining the prior written consent of HKPost, may appoint Subcontractor(s) for the performance of part of the Contract. A list of Subcontractor(s) of Certizen Limited, if any, can be found in **Appendix F**. Certizen Limited, together with its Subcontractor(s) under the Contract, if any, is hereafter referred to as the "Contractor" for the purpose of this CPS.

HKPost remains a Recognized CA under Section 34 of the Ordinance and the Contractor is an agent of HKPost appointed pursuant to Section 3.2 of the Code of Practice for Recognized Certification Authorities issued by the Government Chief Information Officer under Section 33 of the Ordinance.

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

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

It is expedient for HKPost to appoint Registration Authorities (RAs) as its agents to carry out certain of the functions of HKPost as a Recognized CA as set out in this CPS. A list of Registration Authorities, if any, can be found in **Appendix E**.

HKPost is responsible for the conduct and activities of the RAs in carrying out the functions or providing the services of HKPost as its agents as a Recognized CA in respect of the issuing and revocation of e-Certs.

This CPS sets out practices and standards for e-Certs, and the structure of this CPS is as follows:

Section 1	provides 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 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 the certificate, certificate revocation list and online certificate status protocol response profiles
Section 8	documents how this CPS will be administered
Appendix A	contains a glossary
Appendix B	contains formats of e-Certs issued under this CPS
Appendix C	contains formats of HKPost Certificate Revocation List (CRL), Authority Revocation List (ARL) and Online Certificate Status Protocol (OCSP) response
Appendix D	contains a summary of features of e-Certs issued under this CPS
Appendix E	contains a list of HKPost e-Cert Registration Authorities (RAs), if any
Appendix F	contains a list of Subcontractor(s) of Certizen Limited for Hongkong Post e-Cert Services, if any
Appendix G	describes lifespan of CA root certificates
Appendix H	contains a list of particular applications and corresponding application-specific codes for Hongkong Post e-Cert
Appendix I	contains a table of comparison of RFC3647 and this CPS

1. INTRODUCTION

1.1 Overview

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

HKPost shall maintain this CPS in compliance with the Electronic Transactions Ordinance (Cap. 553) and relevant regulations of the Code of Practice for Recognized Certification Authorities ("Code of Practice") of Hong Kong and the relevant regulations of Certificate Policy for Mutual Recognition of Electronic Signature Certificates issued by Hong Kong and Guangdong ("Mutual Recognition Certificate Policy" or "MRCP") under the Arrangement for Mutual Recognition of Electronic Signature Certificates issued by Hong Kong and Guangdong ("Mutual Recognition Arrangement").

The Internet Assigned Numbers Authority ("IANA") has assigned the Private Enterprise Number 16030 to HKPost. For identification purpose, this CPS bears an Object Identifier ("**OID**") **"1.3.6.1.4.1.16030.1.1.36"** (see description of the field "Certificate Policies" in **Appendix B**). Furthermore, as assigned by the Office of the Government Chief Information Officer ("OGCIO"), the OID **"2.16.344.8.2.2008.810.2.2012.1.0**" of the MRCP in company with the OID of this CPS will be specified in the "Certificate Policies" of the e-Cert (Personal) with Mutual Recognition ("MR") Status and the e-Cert (Organisational) with MR Status.

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 making use of a HKPost issued certificate must make an independent determination that PKI based Digital Signatures are appropriate and sufficiently trusted to be used to authenticate the identity of the participants in each Relying Party's particular PKI application.

Under the Ordinance HKPost is a Recognized CA. **HKPost has designated the e-Cert (Personal), e-Cert (Organisational), e-Cert (Server) and e-Cert (Encipherment) certificates issued under this CPS as Recognized Certificates. In particular, the e-Cert (Personal) and e-Cert (Organisational) certificates may incorporate an optional MR feature in compliance with the MRCP, and both of the e-Certs with MR Status are deemed as Recognized Certificates under the Ordinance.** This means for both Subscribers and Relying Parties, that HKPost has a legal obligation under the Ordinance to use a Trustworthy System for the issuance, revocation or suspension, and publication in a publicly available Repository of accepted Recognized Certificates. Recognized Certificates have characteristics of accuracy and contain representations of fact which are defined in law by the Ordinance, including a representation (as further defined below) that such certificates have been issued in accordance with this CPS. The fact that HKPost has appointed Registration Authorities as its agents does not diminish HKPost's obligation to use a Trustworthy System, nor does it alter the characteristics that e-Certs have as Recognized Certificates.

A summary of the features of the certificates issued under this CPS is in **Appendix D**.

1.2 Community and Applicability

1.2.1 Certification Authority

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

1.2.1.1 Representations by HKPost

By issuing a certificate that refers to this CPS, HKPost represents to Relying Parties who act in accordance with Section 2.1.6 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 Section 2.1.6 and other relevant sections of this CPS, that HKPost has issued the certificate to the Subscriber identified in it.

1.2.1.2 Effect

HKPost publishes Recognized Certificates that are accepted by and issued to its Subscribers in a Repository (See Section 2.5).

1.2.1.3 HKPost's Right to Subcontract

HKPost may subcontract its obligations for performing some or all of the functions required by this CPS and the Subscriber Agreement provided that the subcontractor agrees to undertake to perform those functions and enters into a contract with HKPost to perform the services. In the event that such sub-contracting occurs, HKPost shall remain liable for the performance of the CPS and the Subscriber Agreement as if such sub-contracting had not occurred.

1.2.2 End Entities

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

1.2.2.1 Warranties and Representations by Applicants and Subscribers

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

a) No person other than the Subscriber of an e-Cert (Personal) and e-Cert (Server) certificate, the Authorised User of an e-Cert (Organisational) certificate or the Authorised Unit of an e-Cert (Encipherment) certificate has had access to the Subscriber's Private Key.

b) Each Digital Signature generated using the Subscriber's Private Key, which corresponds to the Public Key contained in the Subscriber's e-Cert, is the Digital Signature of the Subscriber.
c) An e-Cert (Server) certificate is to be used only for the purposes stipulated in Section 1.2.3.3 below.
d) An e-Cert (Encipherment) certificate is to be used only for the purposes stipulated in Section 1.2.3.4 below.
e) All information and representations made by the Subscriber included in the certificate are true.
f) The certificate will be used exclusively for authorised and legal purposes consistent with this CPS.
g) All information supplied in the certificate application process does not infringe or violate in any way the trademarks, service marks, trade name, company name, or any other intellectual property rights of any third party.

1.2.3 Classes of Subscribers

HKPost issues certificates under this CPS only to Applicants whose application for a certificate has been approved by HKPost and who have signed or confirmed their acceptance of a Subscriber Agreement in the appropriate form. Four classes of e-Certs are issued under this CPS:

1.2.3.1 e-Cert (Personal) Certificates

An e-Cert (Personal) certificate is issued under this CPS and the Subscriber Agreement to individuals who have a HKID Card. These certificates may be used to perform commercial operations. Meanwhile, an e-Cert (Personal) with MR Status certificate is within the applicable scope under the Mutual Recognition Arrangement as well.

An e-Cert (Personal) certificate may be issued to persons aged under 18 who have a HKID Card (see also Section 3.1.1.2). An e-Cert (Personal) with MR Status certificate shall only be issued to persons aged 18 or above.

1.2.3.2 e-Cert (Organisational) Certificates

An e-Cert (Organisational) certificate is issued to (i) Bureaux and Departments of the Government of Hong Kong SAR, (ii) Organisations that hold a valid business registration certificate issued by the Government of the Hong Kong SAR or a valid certification letter issued by the Inland Revenue Department of the Government of the Hong Kong SAR to the Reporting Financial Institution as referred in the Inland Revenue Ordinance (Cap. 112), and (iii) statutory bodies of Hong Kong whose existence is recognized by the laws of Hong Kong SAR (the "Subscriber Organisation"); and identifies a member or employee whom that Subscriber Organisation has duly authorised to use the Private Key of that e-Cert (Organisational) (the "Authorised User"). These certificates may be used for the same purposes as e-Cert (Personal) certificates. Meanwhile, an e-Cert (Organisational) with MR Status certificate is within the applicable scope under the Mutual Recognition Arrangement as well. An e-Cert (Organisational) with MR Status certificate shall not be issued to persons aged below 18.

SUBSCRIBER ORGANISATIONS, BEING A REPORTING FINANCIAL INSTITUTION AS REFERRED IN THE INLAND REVENUE ORDINANCE (CAP. 112) THAT HOLD A VALID CERTIFICATION LETTER ISSUED BY THE INLAND REVENUE DEPARTMENT OF THE GOVERNMENT OF HONG KONG SAR, UNDERTAKE TO HKPOST NOT TO GIVE AUTHORITY TO THE AUTHORISED USER OF THE E-CERT (ORGANISATIONAL) TO USE THE CERTIFICATE FOR ANY PURPOSE OTHER THAN TO ENCRYPT AND DECRYPT ELECTRONIC MESSAGES, OR GENERATE A

DIGITAL SIGNATURE WITHIN THE PARTICULAR APPLICATION REFERRED TO IN **APPENDIX H**.

1.2.3.3 e-Cert (Server) Certificates

An e-Cert (Server) certificate is issued to Bureaux and Departments of the Government of Hong Kong SAR, Organisations that hold a valid business registration certificate issued by the Government of the Hong Kong SAR and statutory bodies of Hong Kong whose existence is recognized by the laws of Hong Kong SAR (the "Subscriber Organisation"); and that wish to have a certificate issued in a server name, or multiple server names, owned by that Organisation. The left-most component of the fully qualified domain name of the server name may be a wildcard character (i.e. an asterisk character '*') at the discretion of HKPost.

Certificates of this class are to be used for the purposes of conducting enciphered electronic communications and server authentication only. If digital signature Key Usage is enabled in the certificate (referred to in **Appendix B**), the digital signatures supported by the certificates of this class are to be used only for server authentication and for establishment of secure communication channels with the server. The digital signatures generated by this class of certificate are under no circumstances to be used for negotiation or conclusion of a contract or any legally binding agreement or any monetary transactions.

SUBSCRIBER ORGANISATIONS UNDERTAKE TO HKPOST NOT TO GIVE AUTHORITY TO ANY PERSON TO USE A DIGITAL SIGNATURE OF THIS CLASS OF CERTIFICATE OTHER THAN FOR THE PURPOSE OF SERVER AUTHENTICATION OR ESTABLISHMENT OF SECURE COMMUNICATION CHANNELS WITH THE SERVER AND ACCORDINGLY ANY DIGITAL SIGNATURE GENERATED BY THE PRIVATE KEY OF THIS CLASS OF CERTIFICATE USED BY A PERSON OTHER THAN FOR THE AFORESAID PURPOSES MUST BE TREATED AS A SIGNATURE GENERATED AND USED WITHOUT THE AUTHORITY OF THE SUBSCRIBER ORGANISATION WHOSE SIGNATURE IT IS AND MUST BE TREATED FOR ALL PURPOSES AS AN UNAUTHORISED SIGNATURE.

1.2.3.4 e-Cert (Encipherment) Certificates

An e-Cert (Encipherment) certificate is issued to Bureaux and Departments of the Government of Hong Kong SAR, Organisations that hold a valid business registration certificate issued by the Government of Hong Kong SAR and statutory bodies of Hong Kong SAR whose existence is recognized by the laws of Hong Kong SAR (the "Subscriber Organisation"). Such a certificate is designed for use by a unit of the Subscriber Organisation which that Subscriber Organisation has duly authorised to use the Private Key of that e-Cert (Encipherment) certificate (the "Authorised Unit").

Certificates of this class are to be used only:

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

SUBSCRIBER ORGANISATIONS UNDERTAKE TO HKPOST NOT TO GIVE AUTHORITY TO THE AUTHORISED UNITS TO USE A DIGITAL SIGNATURE OF THIS CLASS OF CERTIFICATE FOR ANY OTHER PURPOSE AND ACCORDINGLY ANY DIGITAL SIGNATURE GENERATED BY THE PRIVATE KEY OF THIS CLASS OF CERTIFICATE USED OTHER THAN TO ACKNOWLEDGE RECEIPT OF A MESSAGE AS SET OUT ABOVE MUST BE TREATED AS A SIGNATURE

GENERATED AND USED WITHOUT THE AUTHORITY OF THE SUBSCRIBER ORGANISATION WHOSE SIGNATURE IT IS AND MUST BE TREATED FOR ALL PURPOSES AS AN UNAUTHORISED SIGNATURE.

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

1.2.4 Certificate Lifespan

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

The validity period of certificates issued under this CPS to new Applicants is as follows:

Certificate type	**Validity period specified in the certificate**
e-Cert (Personal)	3 years
e-Cert (Personal) with MR Status	1 year or 2 years or 3 years to be selected by the Applicant at the time of application
e-Cert (Organisational)	1 year or 2 years to be selected by the Applicant at the time of application
e-Cert (Organisational) with MR Status	1 year or 2 years or 3 years to be selected by the Applicant at the time of application
e-Cert (Encipherment)	1 year or 2 years or 3 years or 4 years to be selected by the Applicant at the time of application
e-Cert (Server)	1 year or 2 years to be selected by the Applicant at the time of application
e-Cert (Server) with Wildcard feature or Multi-domain feature	1 year or 2 years to be selected by the Applicant at the time of application

Certificates issued under this CPS as a result of certificate renewal may be valid for a period longer than the respective validity period listed above (see Sections 3.3 and 3.4). The validity period of an e-Cert is specified in the certificate itself. Format of certificates issued under this CPS is in **Appendix B**.

1.2.5 Application at Premises Designated by HKPost

All first applications and applications of a new e-Cert following the revocation or expiration of an e-Cert will require the applicants to submit their applications as described in Sections 3 and 4 of this CPS.

1.3 Contact Details

Subscribers may send their enquiries, suggestions or complaints by:

Mail to : Hongkong Post Certification Authority, Kowloon East Post Office Box 68777
Tel: 2921 6633
Fax: 2775 9130

Email: enquiry@hongkongpost.gov.hk

1.4 Complaints Handling Procedures

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

2. GENERAL PROVISIONS

2.1 Obligations

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

2.1.1 CA Obligations

HKPost, as a Recognized CA, is responsible under the Ordinance for the use of a Trustworthy System for the issuance, revocation, suspension and publication in a publicly available Repository of Recognized Certificates that have been accepted by the Subscriber. In accordance with this CPS, HKPost has the obligation to:

a) issue and publish certificates in a timely manner (see Section 2.5);
b) notify Applicants of the approval or rejection of their applications (see Sections 4.1 to 4.4);
c) suspend or revoke certificates and publish Certificate Revocation Lists and provide OCSP responses in a timely manner (see Section 4.6); and
d) notify Subscribers of the suspension or revocation of their certificates (see Sections 4.6.1, 4.6.2 and 4.6.3).

2.1.2 RA Obligations and Liability

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

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

2.1.3 Contractor Obligations

The Contractor is responsible only to HKPost under the terms of the Contract between HKPost and the Contractor under which the Contractor has been appointed by HKPost as its agent to set up, modify, provide, supply, deliver, operate, administer, promote and maintain the HKPost CA systems and services as stipulated in this CPS. HKPost is and remains

responsible for the activities of the Contractor in the performance or purported performance by the Contractor of the functions, power, rights and duties of HKPost.

2.1.4 Subscriber Obligations

Subscribers are responsible for:

a) Agreeing that the key pair is generated by HKPost in a Trustworthy System and environment within HKPost's premises on behalf of the Subscriber (in the case of applying for an e-Cert (Personal), e-Cert (Organisational) or e-Cert (Encipherment) certificate).
b) Completing the application procedures properly and signing, or confirming acceptance of, a Subscriber Agreement (by the Authorised Representative in the case of applying for an e-Cert (Organisational) certificate, e-Cert (Server) certificate or e-Cert (Encipherment) certificate) in the appropriate form and performing the obligations placed upon them by that Agreement, and ensuring accuracy of representations in certificate application.
c) Accurately following the procedures specified in this CPS as to the expiry of certificates.
d) Acknowledging that they are undertaking an obligation to protect the confidentiality (i.e. keep it secret) and the integrity of their Private Key using reasonable precautions to prevent its loss, disclosure, or unauthorised use, and that they are responsible for any consequences under any circumstances for the compromise of the Private Key.
e) Reporting any loss or compromise of their Private Key immediately to HKPost 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 or of any change in the Authorised User.
g) Notifying HKPost immediately from time to time of any change in the appointment and information of the Authorised Representative in the case of e-Cert (Organisational), e-Cert (Encipherment) and e-Cert (Server) certificates.
h) Notifying HKPost immediately of any fact which may give rise to HKPost, upon the grounds set out in Section 4 below, having the right to revoke the certificate for which that Subscriber is responsible.
i) Agreeing that by having been issued or accepting a certificate they warrant (promise) to HKPost and represent to all Relying Parties that during the operational period of the certificate, the facts stated in Section 1.2.2.1 above are and will remain true.
j) Not using a certificate in a transaction on becoming aware of any ground upon which HKPost could suspend or revoke it under the terms of the CPS, or after the Subscriber has made a revocation request or been notified by HKPost of HKPost's intention to suspend or revoke the certificate under the terms of this CPS.
k) Upon becoming so aware of any ground upon which HKPost could suspend or revoke the certificate, or upon the Subscriber making a revocation request or upon being notified by HKPost of its intention to suspend or revoke the certificate, immediately notifying Relying Parties in any transaction that remains to be completed at the time, that the certificate used in that transaction is liable to be suspended or revoked (either by HKPost or at the Applicant's or Subscriber's request) and stating in clear terms that, as this is the case, the Relying Parties should not rely upon the certificate in respect of the transaction.
l) Acknowledging that by submitting an e-Cert application form, they authorise the publication of the e-Cert to any other person or in the HKPost's Repository.
m) For the purpose of identity authentication, using the Private Key of an e-Cert only during its validity period.

Subscribers of e-Cert (Personal) certificates are also responsible for agreeing to forfeit the use of any Private Keys embedded on the Subscriber's HKID Card in case the Subscriber's HKID Card is lost, destroyed, defaced or damaged, or surrendered to or invalidated or seized by the

Immigration Department or other law enforcement agencies under the laws of the Hong Kong SAR, and that HKPost and the Government of the Hong Kong SAR shall be under no liability to the Applicant or Subscriber in respect of any such events. The Applicant/Subscriber may request HKPost to revoke the e-Cert embedded on the HKID Card in accordance with the procedures stipulated in Section 4.6.2.

Subscribers of e-Cert (Server) certificates are also responsible for ensuring that such certificates are used for the purposes of conducting enciphered electronic communications and server authentication only. If digital signature Key Usage is enabled in the certificate (referred to in **Appendix B**), no attempt is made to use the Private Key relating to an e-Cert (Server) certificate to generate a digital signature other than for the purpose of server authentication or for establishment of secure communication channels with the server.

Subscribers of e-Cert (Encipherment) certificates are also responsible for ensuring that:

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

2.1.5 Subscriber's Liability

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

2.1.6 Relying Party's Obligations

Relying Parties relying upon 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 and any digital signature supported by it is appropriate for its purposes under this CPS while the Contractor or RA (if any, see **Appendix E**) does not undertake any duty of care to Relying Parties at all.

c) Checking the status of the certificate on the certificate revocation list, or the relevant OCSP response whenever applicable, prior to reliance.

d) For e-Cert (Personal) with MR Status and e-Cert (Organisational) with MR Status certificates, checking the official trust list published by the Economic and Information Commission of Guangdong Province to confirm whether the certificate types have valid mutual recognition status and their validity period, a copy of the entries is also maintained in the trust list of the OGCIO for reference, (see Section 2.2.12) prior to reliance.

e) Performing all appropriate certificate path validation procedures.

f) After validity period of the certificate, only using its Public Key for signature verification.

2.2 Further Provisions

Obligations of HKPost to Subscribers and Relying Parties

2.2.1 Reasonable Skill and Care

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

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

This means, for example, that provided that the HKPost, the Contractor or the RA acting on HKPost's behalf has exercised a reasonable degree of skill and care, HKPost, Hong Kong Post Office, the Contractor and any such RA will not be liable for any loss to a Subscriber or Relying Party caused by their 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, the Contractor or the RA acting on behalf of HKPost) has exercised a reasonable degree of skill and care to avoid and/or mitigate the effects of matters beyond its control, neither HKPost, the Hong Kong Post Office, the Contractor nor any such RA is liable for the adverse effects to Subscribers or Relying Parties of any matters outside HKPost's control whatsoever, including (without limitation) the availability of the Internet, or telecommunications or other infrastructure systems or the adverse effects of the acts of God, war, military operations, national emergency, epidemic, fire, flood, earthquake, strike or riots or the negligence or deliberate wrongful conduct of other Subscribers or other third parties.

2.2.2 No Supply of Goods

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

supply of goods. Equally HKPost, in making available the certificates in a public Repository accessible by Relying Parties is not supplying any goods to Relying Parties and likewise gives to Relying Parties no warranty as to the merchantability or fitness for a particular purpose of a certificate nor makes any other representation or warranty as if it were supplying goods to Relying Parties. HKPost agrees to transfer those articles into possession of Applicants or Subscribers for the limited purposes set out in this CPS. Nonetheless HKPost shall exercise reasonable care to see that the same is fit for the purposes of completing and accepting a certificate as set out in this CPS, and if it is not, then HKPost's liability shall be as set out in sections 2.2.3 - 2.2.4 below. In addition, the articles transferred from HKPost may contain other material not relevant to the completion and acceptance of an e-Cert, if it does, the legal position in relation to such material is not governed by the CPS or the Subscriber Agreement, but by separate terms and conditions that will be referred to in the terms and conditions enclosed in the articles.

2.2.3 Limitation of Liability

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

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

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

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

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

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

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

the liability of HKPost to any Subscriber and any Relying Party, whether as Subscriber or Relying Party as defined by the CPS or in any other capacity at all, is limited to, and

shall not under any circumstances exceed, HK$200,000 in respect of one e-Cert (Personal) certificate, e-Cert (Organisational) certificate, e-Cert (Server) certificate or e-Cert (Encipherment) certificate, or HK$0 (zero) in respect of one e-Cert (Personal) certificate issued to a person under 18.

2.2.3.4 Time Limit For Making Claims

Any Subscriber or Relying Party who wishes to make any legal claim upon HKPost arising out of or in any way connected with the issuance, suspension, revocation 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, the Contractor, RAs and their Personnel

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

2.2.3.6 Liability For Wilful Misconduct, Personal Injury or Death

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

2.2.3.7 Certificate Notices, Limitations and Reliance Limit

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

> *"The Postmaster General acting by the officers of the Hong Kong Post Office and the Contractor has issued this certificate as a Recognized CA under the Electronic Transactions Ordinance (Cap. 553) upon the terms and conditions set out in the Postmaster General's Certification Practice Statement (CPS) that applies to this certificate.*
>
> *Accordingly, any person, before relying upon this certificate should read the CPS that applies to e-Certs which may be read on the HKPost CA web site at www.hongkongpost.gov.hk. The laws of Hong Kong SAR apply to this certificate and Relying Parties must submit any dispute or issue arising as a result of their reliance upon this certificate to the non-exclusive jurisdiction of the Courts of Hong Kong SAR.*

If you, as a Relying Party, do not accept the terms and conditions upon which this certificate is issued, then do not rely upon it.

The Postmaster General (by the Hong Kong Post Office, the Contractor and their respective officers, employees and agents) 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 and any digital signature supported by it is appropriate for its purposes under the CPS;*
c. *Checking the status of this certificate on the Certificate Revocation List, or the relevant OCSP response whenever applicable, prior to reliance; and*
d. *Performing all appropriate certificate path validation procedures.*

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

If this certificate is in any way inaccurate or misleading and this is the result of the negligence of the Postmaster General, Hong Kong Post Office, the Contractor or their respective officers, employees or agents, then the Postmaster General will pay a Relying Party up to HK$200,000, or HK$0 if this certificate is an e-Cert (Personal) certificate issued to a person under 18, in respect of proved loss caused by reasonable reliance upon such inaccurate or misleading matters in this certificate where such losses are not and do not include (1) any direct or indirect loss of profits or revenue, loss or injury to reputation or goodwill, loss of any opportunity or chance, loss of projects, or the loss or loss of use of any data, equipment or software or (2) any indirect, consequential or incidental loss or damage even if, in respect of the latter, HKPost has been advised of the likelihood of such loss or damage in advance. The applicable Reliance Limit that applies to this certificate under the Ordinance in these circumstances is HK$200,000, or HK$0 if this certificate is an e-Cert (Personal) certificate issued to a person under 18, and in all cases in relation to categories of loss (1) and (2), is HK$0.

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

<u>Time Limit For Making Claims</u>
Any Relying Party who wishes to make any legal claim upon the Postmaster General arising out of or in any way connected with the issuance, suspension, revocation 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, the Contractor and their officers, employees or agents, this certificate does not impose any limit upon their liability to Relying Parties who suffer loss in consequence of reasonable reliance upon such misrepresentations in this certificate.

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

2.2.4 HKPost's Liability for Received but Defective Certificates

Notwithstanding the limitation of HKPost's liability set out above, if, after receiving the certificate, a Subscriber finds that, because of any error in the Private Key or Public Key of the certificate, no transactions contemplated by the PKI can be completed properly or at all, and that Subscriber notifies HKPost of this immediately to permit the certificate to be revoked and (if desired) re-issued, then, if such notification has occurred within 3 months after receiving the certificate and the Subscriber no longer wants a certificate, HKPost, on being satisfied of the existence of any such error will refund the fee paid. If the Subscriber waits longer than 3 months after receiving the certificate before notifying HKPost of any such error, the fee paid will not be refunded as of right, but only at the discretion of HKPost.

2.2.5 Assignment by Subscriber

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

2.2.6 Authority to Make Representations

Except as expressly authorised by HKPost, no agent or employee of the Hong Kong Post Office, the Contractor or of any RA has authority to make any representations on behalf of HKPost as to the meaning or interpretation of this CPS.

2.2.7 Variation

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

2.2.8 Retention of Title

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

2.2.9 Conflict of Provisions

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

2.2.10 Fiduciary Relationships

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

2.2.11 Cross Certification

In all instances in relation to the e-Cert (Personal), e-Cert (Organisational), e-Cert (Encipherment) and e-Cert (Server) certificates issued under this CPS, HKPost reserves the right to define and determine suitable grounds for cross-certification with another CA.

For the e-Cert (Personal) with MR Status and e-Cert (Organisational) with MR Status certificates issued under this CPS and in compliance with the MRCP, HKPost may abandon the right to define and determine suitable grounds for cross-certification with another CA.

2.2.12 Trust List of Mutual Recognition Certificates

HKPost has designated the e-Cert (Personal) with MR Status and the e-Cert (Organisational) with MR Status to participate in the mutual recognition scheme under the Mutual Recognition Arrangement. For the specific certificate types with mutual recognition status and the verification method of these certificate types, please refer to the official trust list published by the Economic and Information Commission of Guangdong Province to confirm whether the certificate types have valid mutual recognition status and their validity period. A copy of the entries is also maintained in the trust list of the OGCIO for reference.

2.2.13 Disclaimer of Mutual Recognition Certificates

On the basis of compliance with the local legal regulatory requirements and the MRCP, HKPost, Subscribers and Relying Parties shall not take actions against the governments of Hong Kong and Guangdong as well as the competent authorities of certification services of the two places for any liabilities and claims for compensation arising from the deficiencies or negligence of HKPost or the e-Cert (Personal) with MR Status or e-Cert (Organisational) with MR Status certificates.

2.2.14 Concerning the Comparison of the Scope of Contents of this CPS with the RFC3647 Standard

This CPS and the MRCP are written with reference to the RFC2527 and RFC3647 standards respectively. In consideration of the current format of this CPS that has been adopted by subscribers and relying parties, and other relevant parties for a long period of time, a substantial change to the format of the current CPS to cope with the requirement as specified in Section IV. 1. (3) of the MRCP for the issuance of e-Cert (Personal) and e-Cert (Organisational) certificates for participation in the mutual recognition scheme of certificates under the "Arrangement of mutual recognition of electronic signature certificates issued by Hong Kong and Guangdong" may cause confusion in the understanding of the CPS by subscribers and relying parties, and other relevant parties. In view of this, it is therefore determined that a comparison table of the CPS outline of Request for Comments ("RFC") 3647 with the corresponding sections of this CPS be provided in **Appendix I** to serve the same purpose for the time being.

2.2.15 Financial Responsibility

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

2.3 Interpretation and Enforcement (Governing Law)

2.3.1 Governing Law

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

2.3.2 Severability, Survival, Merger, and Notice

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

2.3.3 Dispute Resolution Procedures

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

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

2.3.4 Interpretation

Where there is a conflict of interpretation of wording between the English and Chinese versions of this CPS, the English version shall prevail. If, for any clause applicable to the e-Cert (Personal) with MR Status or e-Cert (Organisational) with MR Status, there is a conflict of interpretation of wording between the English and Chinese versions of this CPS, the Traditional Chinese version shall prevail.

2.4 Subscription Fees

The subscription fee and administration fee shall be paid before the commencement of each subscription period (see section 3.2) by e-Cert Subscribers unless waived by HKPost. HKPost may suspend or revoke an e-Cert if its subscription terminates during the validity period specified in the certificate (see also section 4.6.1.4(f)). HKPost reserves its absolute right to review and determine the subscription fee and administration fee from time to time and will notify the Subscribers and the public at the HKPost web site http://www.hongkongpost.gov.hk. Under the terms of the Contract between HKPost and Certizen Limited, Certizen Limited is entitled to receive subscription, renewal and administration fees from e-Cert Subscribers.

2.4.1 e-Cert (Personal) Certificates

The subscription fee for an e-Cert (Personal) certificates (for both first time application and renewal) is HK$50 per certificate per year.

Subscription fees for e-Cert (Personal) with MR Status certificates are as follows:

Subscription Fees for e-Cert (Personal) with MR Status Certificates	**Certificate with a 1-year validity period**	**Certificate with a 2-year validity period**	**Certificate with a 3-year validity period**
First time application and renewal	HK$50 per certificate	HK$100 per certificate	HK$150 per certificate
e-Cert Storage Medium	Each e-Cert can be stored in Smart ID Card for free or a specified e-Cert Storage Medium with an extra fee. Latest price of the e-Cert Storage Medium shall be published in the website of HKPost at http://www.hongkongpost.gov.hk.		

2.4.2 e-Cert (Organisational) Certificates

<table>
<tr><th colspan="2">Subscription Fees for e-Cert (Organisational) Certificates</th><th>Certificate with a 1-year validity period</th><th>Certificate with a 2 – year validity period</th><th>Certificate with a 3-year validity period</th></tr>
<tr><td rowspan="5">Without MR Status</td><td>First time application</td><td>HK$50 per certificate</td><td>HK$200 per certificate</td><td rowspan="5">Not applicable</td></tr>
<tr><td>Non-first time application or renewal</td><td>HK$150 per certificate</td><td>HK$300 per certificate</td></tr>
<tr><td rowspan="3"></td><td colspan="2" rowspan="2">Promotional discount on subscription fees for e-Cert (Organisational) certificates is offered by the Contractor. For details on the promotional discount, please refer to HKPost web site at http://www.hongkongpost.gov.hk or make enquiry to Hongkong Post Certification Authority through the means provided in Section 1.3.</td></tr>
<tr><td rowspan="2">Administration fee (irrespective of the number of Authorised Users)</td></tr>
<tr><td>HK$150
per application</td><td>HK$300
per application</td></tr>
<tr><td rowspan="4">With MR Status</td><td>New application or renewal</td><td>HK$150 per certificate</td><td>HK$300 per certificate</td><td>HK$450 per certificate</td></tr>
<tr><td rowspan="2">Administration fee (irrespective of the number of Authorised Users)</td><td>HK$150
per application</td><td>HK$300
per application</td><td>HK$450
per application</td></tr>
<tr><td colspan="3">If the application form contains applications for certificates with multiple certificate validity periods, the administration fee is calculated based on the applied certificate with the longest validity period.</td></tr>
<tr><td>e-Cert Storage Medium</td><td colspan="3">Each e-Cert must be separately stored in a specified e-Cert Storage Medium. Latest price of the e-Cert Storage Medium shall be published in the website of HKPost at http://www.hongkongpost.gov.hk.</td></tr>
</table>

2.4.3 e-Cert (Server) Certificates

<table>
<tr><th>Subscription Fees per certificate for e-Cert (Server) Certificates</th><th>Certificate with a 1-year validity period</th><th>Certificate with a 2-year validity period</th></tr>
<tr><td rowspan="2">New application or renewal without Wildcard feature or Multi-domain feature</td><td>HK$2,500</td><td>HK$5,000</td></tr>
<tr><td colspan="2">Promotional discount on subscription fees for e-Cert (Server) certificates is offered by the Contractor. For details on the promotional discount, please refer to HKPost web site at http://www.hongkongpost.gov.hk or make enquiry to Hongkong Post Certification Authority through the means provided in Section 1.3.</td></tr>
</table>

New application or renewal with Wildcard feature	HK$8,700 + HK$500 per additional server	HK$17,400 + HK$1,000 per additional server
	Certificates with Wildcard feature can be used in one server by default. Extra fee per additional server applies if it is to be used in more than one server, and that the extra fee per additional server shall be applied for the whole validity period of the certificate regardless of when the certificate is to be used in the additional servers.	
New application or renewal with Multi-domain feature	HK$3,000 + HK$2,500 per additional server name	HK$6,000 + HK$5,000 per additional server name
	Certificates with Multi-domain feature identify one server name by default. Extra fee per additional server name applies if more than one, but not more than 50, server names are to be identified in the certificate.	

2.4.4 e-Cert (Encipherment) Certificates

Subscription Fees for e-Cert (Encipherment) Certificates	**Certificate with a 1-year validity period**	**Certificate with a 2-year validity period**	**Certificate with a 3-year validity period**	**Certificate with a 4-year validity period**
New application or renewal	HK$150 per certificate	HK$300 per certificate	HK$450 per certificate	HK$600 per certificate
	Promotional discount on subscription fees for e-Cert (Encipherment) certificates is offered by the Contractor. For details on the promotional discount, please refer to HKPost web site at http://www.hongkongpost.gov.hk or make enquiry to Hongkong Post Certification Authority through the means provided in Section 1.3.			
Administration fee (irrespective of the number of Authorised Units)	HK$150 per application	HK$300 per application	HK$450 per application	HK$600 per application
	If the application form contains applications for certificates with multiple certificate validity periods, the administration fee is calculated based on the applied certificate with the longest validity period.			

2.5 Publication and Repository

Under the Ordinance, HKPost maintains a Repository that contains a list of accepted certificates issued under this CPS, the current certificate revocation list, the current OCSP responses, the HKPost Public Key, a copy of this CPS, and other Information related to e-Cert certificates which reference this CPS, such as e-Cert application forms and the "Subscribers Terms and Conditions" enclosed in the application forms. This CPS and the latest version of "Subscribers Terms and Conditions" shall constitute the pubic Subscriber Agreement and Relying Party Agreement. HKPost shall promptly publish and update the Repository regarding the relevant disclosed documents and disclosure records of the previously published documents and their amendments. The Repository is available on a substantially 24 hours per day, 7 days per week basis, subject to scheduled maintenance of an average of 2 hours per week and any emergency maintenance. HKPost promptly publishes each certificate accepted

by and issued to the Subscriber under this CPS in the Repository. The HKPost Repository can be accessed at URLs as follows:

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

2.5.1 Certificate Repository Controls

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

2.5.2 Certificate Repository Access Requirements

Only persons authorised by HKPost have access to the Repository to update and modify the contents. In operating and maintaining the Repository, HKPost shall not carry out any activities that may create unreasonable risk to persons relying on the Repository (including the certificates and other information).

2.5.3 Certificate Repository Update Cycle

The Repository is updated promptly after each certificate is accepted by and issued to the Subscriber and any other applicable events such as update of certificate revocation list and provision of OCSP responses.

2.5.4 Permitted Use of Information Contained in the Repository

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

2.6 Compliance Assessment

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

2.7 Confidentiality

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

3. IDENTIFICATION AND AUTHENTICATION

3.1 Initial Application

In respect of e-Cert (Personal) certificate applications, each Applicant (save in the case of Applicants who are holders of valid e-Cert (Personal) certificates) must appear in person at a designated HKPost premises, or premises of other organisations designated by HKPost, and present proof of identity face-to-face as described in section 3.1.9. In the case of Applicants who are holders of valid e-Cert (Personal) certificates, their attendance is not required, but their valid Digital Signatures supported by their e-Cert (Personal) certificates are required as proof of identity.

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

All Applicants for e-Certs shall submit a completed and signed application form to HKPost. The e-Cert (Organisational) certificate, e-Cert (Server) certificate and e-Cert (Encipherment) certificate applications require the Authorised Representative of the Organisation to complete and sign the application form and the Organisation will become a Subscriber. Following approval of the application, HKPost prepares an e-Cert and notifies the Applicant of how the certificate may be issued.

3.1.1 Types of Names

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

3.1.1.2 e-Cert (Personal) certificates issued to Subscribers who are under 18
For an e-Cert (Personal) certificate without MR Status, the Subscriber is identified in the certificate with a Subject Name specified in Section 3.1.1.1 and the wording "e-Cert (Personal/Minor)" (see **Appendix B**) to indicate that the Subscriber is under 18 at the time the certificate is issued.

3.1.1.3 e-Cert (Organisational) certificates
The Subscriber Organisation for an e-Cert (Organisational) certificate is identified in the certificate with a Subject Name (referred to in **Appendix B**) consisting of:

a) The Authorised User's name as it appears on the Authorised User's HKID Card/passport;
b) The Subscriber Organisation's name as it is registered with the appropriate Hong Kong registration agency or a Bureau/Department of the Government of the Hong Kong SAR or as a statutory body whose existence is recognized by the laws of Hong Kong SAR, or the official name of that Bureau or Department where the Subscriber Organisation is a Bureau or Department of the Government of Hong Kong SAR; and
c) The Subscriber Organisation's Hong Kong Company/Business Registration Number, or the Subscriber Organisation's IRD Reference Number, where the Subscriber Organisation is not a Bureau or Department of the Government of Hong Kong SAR or as a statutory body whose existence is recognized by the laws of Hong Kong SAR.

3.1.1.4 e-Cert (Server) certificates

The Subscriber Organisation for an e-Cert (Server) certificate is identified in the certificate with a Subject Name (referred to in **Appendix B**) consisting of:

a) The Subscriber Organisation's name as it is registered with the appropriate Hong Kong registration agency or a Bureau/Department of the Government of the Hong Kong SAR or as a statutory body whose existence is recognized by the laws of Hong Kong SAR, or the official name of that Bureau or Department where the Subscriber Organisation is a Bureau or Department of the Government of Hong Kong SAR;
b) The Subscriber Organisation's Hong Kong Company/Business Registration Number where the Subscriber Organisation is not a Bureau or Department of the Government of Hong Kong SAR or a statutory body whose existence is recognized by the laws of Hong Kong SAR; and
c) The server name (including domain name of the server) owned by the Subscriber Organisation. The left-most component of the fully qualified domain name of the server name may be a wildcard character (i.e. an asterisk character '*', the wildcard component) at the discretion of HKPost, meaning that the certificate may be used for all server names at the same domain or sub-domain level owned by the Subscriber Organisation.

For Subscriber Organisation who applied for an e-Cert (Server) certificate with either Wildcard feature or Multi-domain feature, the e-Cert (Server) certificate will contain a Subject Alternative Name (referred to in **Appendix B**) consisting of the server name (including domain name of the server) owned by the Subscriber Organisation identified in the Subject Name. For an e-Cert (Server) with Wildcard feature, the Subject Alternative Name will also include the server name without the wildcard component of the applied server name owned by the Subscriber Organisation. For an e-Cert (Server) with Multi-domain feature, there may be additional server name(s) in the Subject Alternative Name, and each additional server name must be owned by the Subscriber Organisation. No wildcard character (i.e. an asterisk character '*') will be allowed in any part of the additional server name(s).

3.1.1.5 e-Cert (Encipherment) certificates

The Subscriber Organisation for an e-Cert (Encipherment) certificate is identified in the certificate with a Subject Name (referred to in **Appendix B**) consisting of:

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

3.1.1.6 The Authorised Representative

Although the Authorised Representative of the Subscriber Organisation is responsible for administering on behalf of the Subscriber Organisation the application for an e-Cert (Organisational) certificate, e-Cert (Server) certificate or e-Cert (Encipherment) certificate, that person will not be identified in the e-Cert.

3.1.1.7 Organisation Names in Chinese Language

e-Cert (Personal), e-Cert (Encipherment) and e-Cert (Server) are issued in English language only. For Organisations who subscribe to e-Cert (Encipherment) or e-Cert (Server) and are companies with company names in the Chinese language only or who have provided their company's Chinese name only, their company names will not be displayed on the e-Cert.

e-Cert (Organisational) are issued in English language but will contain also the organisation name and branch name in Chinese language, when the Organisation has provided the respective Chinese names in the application form. For Organisations who subscribe to e-Cert (Organisational) and are companies with company names in the Chinese language only, a default name "***CHINESE NAME ONLY***" will be set for the company's English name.

3.1.2 Need for Names to be Meaningful

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

3.1.3 Rules for Interpreting Various Names

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

3.1.4 Name Uniqueness

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

3.1.5 Name Claim Dispute Resolution Procedure

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

3.1.6 Infringement and Violation of Trademarks

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

3.1.7 Method to Prove Possession of the Private Key

HKPost carry out the central key generation service on behalf of the Subscriber. HKPost shall generate the certificate in a Trustworthy System and environment within HKPost's premises to ensure that the Private Key is not tampered with. The Private Key together with the certificate will be stored on an e-Cert Storage Medium and delivered to the Applicant in a secure manner stipulated in sections 4.1, 4.2, 4.3 and 4.4 below.

3.1.8 Authentication of Identity of Organisational Applicant

3.1.8.1 Applications for e-Cert (Organisational), e-Cert (Server) and e-Cert (Encipherment) certificates should be made at a designated HKPost premises, or premises of other organisations designated by HKPost by the personal attendance of the Applicant's Authorised Representative who is required to present his/her own HKID Card or passport. At the sole discretion of HKPost, it may be permitted for submission of the application accompanied by a copy of the Authorised Representative's own HKID Card or passport with the Authorised Representative's signature, in lieu of the Authorised Representative's personal attendance, provided that (a) the Authorised Representative's identity has been authenticated in a past application of the Subscriber Organisation, and the Authorised Representative has appeared at the designated HKPost premises, or premises of other organisations designated by HKPost for

identity verification in that application; and (b) reasonable justification is available for re-affirming the identity of the Authorised Representative, such as confirmation with the Authorised Representative through telephone call or checking the Authorised Representative's signature against that on past application records. In case of doubt, HKPost may decline the application.

3.1.8.2 Each application for e-Cert (Organisational) certificates must be accompanied by the following documentation:

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

3.1.8.3 Each application for e-Cert (Server) certificates must be accompanied by the following documentation:

a) An authorisation letter bearing the "For and on behalf of" chop and the authorised signature(s) of the Organisation giving authority to the Authorised Representative to make the application and prove the ownership of the domain name(s) to be identified in the Subject Name and Subject Alternative Name, if any, in the e-Cert (Server) certificate; and
b) Documentation issued by the appropriate Hong Kong registration agency attesting the existence of the Organisation. The validity of the documentation should not expire within one month by the time the application is submitted;

3.1.8.4 Each application for e-Cert (Encipherment) certificates must be accompanied by the following documentation:

a) An authorisation letter bearing the "For and on behalf of" chop and the authorised signature(s) of the Organisation giving authority to the Authorised Representative to make the application; and
b) Documentation issued by the appropriate Hong Kong registration agency attesting the existence of the Organisation. The validity of the documentation should not expire within one month by the time the application is submitted;

3.1.8.5 Applications from Bureaux or Departments of the Government of Hong Kong SAR, must be accompanied by a memo, a letter or a relevant application form impressed with the relevant Bureau or Department chop, appointing the Authorised Representative to sign on behalf of the Bureau or Department, any documents relating to the application, revocation and renewal of HKPost e-Certs. The memo, letter or relevant application form must be signed by a Departmental Secretary or officer at equivalent level or above.

3.1.8.6 For Subscriber Organisations to whom an e-Cert (Organisational), e-Cert (Encipherment) or e-Cert (Server) certificate with more than one year of validity period is issued, HKPost shall verify again the existence of the Subscriber Organisation, and in the case

of e-Cert (Server) the ownership of the domain name(s) identified in the certificate, approximately at the end of each anniversary date of the e-Cert during the validity period. HKPost may suspend or revoke the certificates issued to that Subscriber Organisation in accordance with the provisions set out in Section 4.6 (Certificate Suspension and Revocation) of this CPS if the Subscriber Organisation's existence cannot be attested, or in the case of e-Cert (Server) the ownership of the domain name(s) cannot be attested.

3.1.9 Authentication of Identity of Personal Applicant

Confirmation of the identity of each Applicant of e-Cert (Personal) certificate will be accomplished through one of the following processes:

a) Each Applicant for a certificate shall appear at a designated HKPost premises, or premises of other organisations designated by HKPost, and submit a completed and signed e-Cert application form and the Subscriber Agreement and the Applicant's HKID Card. Personnel at the aforementioned premises will review and certify the application package face-to-face, and forward the application to HKPost CA Centre for processing.
b) Each Applicant for a certificate shall present his valid Digital Signature supported by a valid e-Cert (Personal) certificate. Applicants without a valid e-Cert (Personal) certificate should follow the process at (a) above for identity confirmation.
c) In case of doubt, HKPost may decline the application.

3.2 Subscription Period of e-Cert (Personal) Certificates

3.2.1 The e-Cert (Personal) certificate without MR Status is valid for three years and its subscription period is one year. HKPost shall notify the Subscriber to extend the subscription period prior to its expiry. The subscription of e-Cert service can be extended before expiry of the subscription period at the request of the Subscriber, the discretion of HKPost, or upon special promotional program introduced by HKPost. HKPost shall not perform extension of subscription period for expired or revoked certificates. The e-Cert (Personal) with MR Status certificate is valid for one year or two years or three years (see Section 1.2.4); the subscription period shall be the same as its validity period and the relevant arrangement of the extension of subscription period is not applicable.

3.2.2 For the e-Cert (Personal) certificate without MR Status, the Subscriber will not be issued another e-Cert (Personal) certificate upon extension of subscription period during the three-year validity period. If a Subscriber does not pay the subscription fee when required before the subscription period expires, his e-Cert may be revoked upon expiry of subscription period. In the case of e-Cert (Personal) certificate embedded in Smart ID Card (see Section 4.1), the Subscriber may leave the e-Cert on the Smart ID Card or go to one of the designated Post Offices to have his e-Cert removed from the Smart ID Card.

3.2.3 The subscription period of an e-Cert (Personal) certificate without MR Status may be extended without going through the process of an authentication of the identity of the Subscriber which is required when a new certificate application is made. To request for extension of the subscription period, the Subscriber is required to settle the payment by such means as HKPost shall from time to time stipulate. HKPost may, at its discretion, extend the subscription period of the Subscriber without asking the Subscriber to request for the extension of the subscription period. Upon extension of the subscription period, the Subscriber's e-Cert and key pair will continue to be valid and generation of new key pair of the Subscriber will not be required. Upon extension of the subscription period, the terms and conditions of the original Subscriber Agreement will apply to the certificate, except insofar as such terms are incompatible with the terms of the CPS current at the date of the extension of

subscription period. In the case of such incompatibility the terms of the current CPS will prevail. Upon extension of the subscription period, the Subscriber should read the terms of the CPS current at the date of the request.

3.3 Renewal of e-Cert (Personal) Certificates

3.3.1 HKPost shall notify Subscribers to renew their e-Cert (Personal) certificates prior to the expiry of the certificates' validity period. The certificates can be renewed before expiry of their validity at the request of the Subscriber and the discretion of HKPost. HKPost shall not perform renewal of expired, suspended or revoked certificates. At the discretion of HKPost, the validity period of the new certificate to be issued to the Subscriber may be valid for a period longer than the validity period of the certificate specified in Section 1.2.4:

For the e-Cert (Personal) certificate without MR Status:

Validity period of a new certificate[1]	**Validity period start date to be specified in the new certificate**	**Validity period end date to be specified in the new certificate**	**Remarks**
Three years	The date the new certificate is generated	The date that is three years after the expiry date of the old certificate being renewed	The new certificate may have a validity period of more than three years but no more than three years and one month

For the e-Cert (Personal) with MR Status certificate:

Validity period of a new certificate[1]	**Validity period start date to be specified in the new certificate**	**Validity period end date to be specified in the new certificate**	**Remarks**
One year	The date the new certificate is generated	The date that is one year after the expiry date of the old certificate being renewed	The new certificate may have a validity period of more than one year but no more than one year and one month
Two years	The date the new certificate is generated	The date that is two years after the expiry date of the old certificate being renewed	The new certificate may have a validity period of more than two years but no more than two years and one month
Three years	The date the new certificate is generated	The date that is three years after the expiry date of the old certificate being renewed	The new certificate may have a validity period of more than three years but no more than three years and one month

3.3.2 By using valid digital signature as specified in section 3.1.9 (b), an e-Cert (Personal) certificate may be renewed without going through the process of an authentication of the identity of the Subscriber which is required when a new certificate application is made. Other

[1] See Section 1.2.4

than that, the Subscriber is required to submit a completed and signed renewal application form to HKPost to apply for renewal. Details of the renewal application are available at both post offices and HKPost's web site at http://www.hongkongpost.gov.hk. Upon certificate renewal, a new key pair of the Subscriber will be generated through HKPost's central key generation service. Upon certificate renewal, the terms and conditions of the original Subscriber Agreement will apply to the renewed certificate, except insofar as such terms are incompatible with the terms of the CPS current at the date of renewal. In the case of such incompatibility the terms of the current CPS will prevail. Applicants for renewal should read the terms of the CPS current at the date of renewal before submitting the renewal forms.

3.4 Renewal of e-Cert (Organisational), e-Cert (Server) and e-Cert (Encipherment) Certificates

3.4.1 HKPost shall notify Subscribers to renew their e-Cert (Organisational), e-Cert (Server) and e-Cert (Encipherment) certificates prior to the expiry of the certificates. The certificates can be renewed before expiry of their validity at the request of the Subscriber and the discretion of HKPost. HKPost shall not perform renewal of expired, suspended or revoked certificates. At the discretion of HKPost, the validity period of the new certificate to be issued to the Subscriber may be valid for a period longer than the validity period of the certificate specified in Section 1.2.4:

Validity period of a new certificate[1]	**Validity period start date to be specified in the new certificate**	**Validity period end date to be specified in the new certificate**	**Remarks**
One year	The date the new certificate is generated	The date that is one year after the expiry date of the old certificate being renewed	The new certificate may have a validity period of more than one year but no more than one year and one month
Two years	The date the new certificate is generated	The date that is two years after the expiry date of the old certificate being renewed	The new certificate may have a validity period of more than two years but no more than two years and one month
Three years[2]	The date the new certificate is generated	The date that is three years after the expiry date of the old certificate being renewed	The new certificate may have a validity period of more than three years but no more than three years and one month
Four years[3]	The date the new certificate is generated	The date that is four years after the expiry date of the old certificate being renewed	The new certificate may have a validity period of more than four years but no more than four years and one month

3.4.2 There is no automatic certificate renewal of an e-Cert (Organisational), e-Cert (Server) and e-Cert (Encipherment) certificates. The process of "Authentication of Identity of

[1] See Section 1.2.4
[2] For e-Cert (Organisational) with MR Status, and e-Cert (Encipherment) only
[3] For e-Cert (Encipherment) only

Organisational Applicant" as described under Section 3.1.8 will be conducted. The Authorised Representative of the Organisation will need to complete and submit a Certificate Renewal Form (available at HKPost web site at http://www.hongkongpost.gov.hk) along with the other documentation referred to in the application form and appropriate renewal fee. In circumstances where Authorised Representatives are replaced, the new Authorised Representative will need to also complete and submit an application form.

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

4. OPERATIONAL REQUIREMENTS

4.1 e-Cert (Personal) Certificates

4.1.1 Certificate Application

4.1.1.1 Application Processing

4.1.1.1.1 Applicants for e-Cert (Personal) certificate under this CPS must complete and submit an application on a form agreed by HKPost at a designated HKPost premises or premises of other organisations designated by HKPost.

4.1.1.1.2 For an e-Cert (Personal) certificate without MR Status, the Applicant, at the time of application, may choose an e-Cert Storage Medium for issuance of the e-Cert and the Private Key. The Applicant may apply to embed the e-Cert and Private Key on the Smart ID Card at designated HKPost premises in addition to issuance of e-Cert and the Private Key in the selected e-Cert Storage Medium.

For an e-Cert (Personal) with MR Status certificate, the Applicant, at the time of application, can only choose the designated PKCS#11 compatible e-Cert Storage Medium for issuance of the e-Cert and the Private Key, or apply to embed the e-Cert and Private Key on the Smart ID Card at designated HKPost premises.

4.1.1.1.3 For an e-Cert (Personal) certificate without MR Status, the Applicant may, at the time of submitting an application form, request an additional copy of the e-Cert and the Private Key to be stored in Alternative Storage Medium that is provided by the Applicant. If HKPost considers the request acceptable, HKPost shall store the additional copy of the e-Cert and the Private Key in each of the Alternative Storage Medium. In such case, the process in Section 4.1.2 is also applicable to the additional copy of the e-Cert and the Private Key. In particular, the additional copy of the e-Cert and the Private Key will be protected by e-Cert PIN and delivered to the Applicant in a secure manner.

4.1.1.1.4 HKPost has implemented internal procedures and controls over the preparation, activation, usage, distribution and termination of any key storage media. The procedures and controls are regularly reviewed by independent third party.

4.1.1.1.5 By submitting an e-Cert application form, the Applicant authorises the publication of the e-Cert to any other person or in the HKPost Repository and accepts the e-Cert to be issued to the Applicant.

4.1.1.2 Identity Verification

4.1.1.2.1 The Applicant is required to present his HKID Card for identity verification conducted by personnel of HKPost or its agents at designated HKPost premises or premises of other organisations designated by HKPost as stated in section 3.1.9 (a). Upon satisfactory completion of the identity verification process, an e-Cert PIN envelope will be delivered to the Applicant.

4.1.1.2.2 Each of the e-Certs and Private Keys embedded onto the Smart ID Cards will be protected by individual PINs. The PINs will be distributed to the e-Cert Applicants separately in the form of sealed PIN envelopes. The e-Cert PIN will be required for any

subsequent use of the e-Cert and Private Key in order to prevent unauthorised access to the e-Cert and Private Key.

4.1.2 Issuance of e-Cert (Personal) Certificate and Publication

4.1.2.1 Issuing and Embedding e-Cert (Personal) Certificate onto Smart ID Cards at Designated HKPost Premises

4.1.2.1.1 Applicants who hold a Smart ID Card capable for embedment of an e-Cert with 2048-bit RSA key length and decide to opt for embedding an e-Cert and the Private Key in their Smart ID Cards in addition to the issuance of the e-Cert and the Private Key in the selected e-Cert Storage Medium, they may complete their applications and embed their e-Certs and Private Keys on their Smart ID Cards (See Section 4.1.1.1.2) over the designated HKPost premises (the list is published at the HKPost web site at http://www.hongkongpost.gov.hk) through the following steps:

a) The Applicant submits the application, completes identity verification and collects the PIN envelope in accordance with the process described in Section 4.1.1.1 and 4.1.1.2.

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

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

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

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

f) For an e-Cert (Personal) certificate without MR Status, the Private Key and e-Cert will be stored on the e-Cert Storage Medium and the Alternative Storage Medium, if any, selected by the Applicant. Each of the e-Certs and Private Keys embedded onto the e-Cert Storage Medium and the Alternative Storage Medium, if any, will be protected by the e-Cert PIN in the Applicant's PIN envelope. The e-Cert PIN will be required for any subsequent use of the e-Cert and Private Key in order to prevent unauthorised access to the e-Cert and Private Key. The e-Cert Storage Medium and the Alternative Storage Medium, if any, which will be sealed up in a tamper-proof envelope or other forms of containers, will then be delivered to the Applicant in a secure manner such as by registered mail.

g) The accepted and issued e-Cert will then be published in the HKPost Repository.

4.1.2.2 Issuance of e-Cert in e-Cert Storage Medium and Alternative Storage Medium

4.1.2.2.1 Applicants may complete their application at designated HKPost premises, or premises of other organisations designated by HKPost, and collect their e-Certs and Private Keys stored on the e-Cert Storage Medium and the Alternative Storage Medium, if any, selected by the Applicant by post through the following steps:

a) The Applicant presents his HKID Card for identity verification conducted by personnel of HKPost or its agents at designated HKPost premises or premises of other organisations designated by HKPost as stated in section 3.1.9 (a). Upon satisfactory completion of the identity verification process, an e-Cert PIN envelope will be delivered to the Applicant.

b) Following the identity verification process, HKPost shall generate the e-Certs (including the associated key pairs) of the respective Applicants in a Trustworthy System and environment within HKPost's premises to ensure that the Private Key will not be tampered with.

c) The Private Key and e-Cert will then be stored on the e-Cert Storage Medium and the Alternative Storage Medium, if any, selected by the Applicant. Each of the e-Certs and Private Keys embedded onto the e-Cert Storage Medium and the Alternative Storage Medium, if any, will be protected by the e-Cert PIN in the Applicant's PIN envelope. The e-Cert PIN will be required for any subsequent use of the e-Cert and Private Key in order to prevent unauthorised access to the e-Cert and Private Key. The e-Cert Storage Medium and the Alternative Storage Medium, if any, which will be sealed up in a tamper-proof envelope or other forms of containers, will then be delivered to the Applicant in a secure manner such as by registered mail.

d) The accepted and issued e-Cert will then be published in the HKPost Repository.

4.1.2.3 Private Keys

4.1.2.3.1 The e-Cert and the Private Key embedded on the Smart ID Card shall not be recovered in case the card is lost or damaged. As such, the Applicant shall keep his e-Cert and the Private Key stored on the e-Cert Storage Medium or Alternative Storage Medium, if any, as backup of his e-Cert and Private Key embedded on the Smart ID Card.

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

4.1.2.4 Verification on Certificate Information

Applicants can either verify the information on the certificate by browsing the certificate file or through HKPost CA Repository. Applicants can also verify the information of certificate that was embedded on the Smart ID Card by applying appropriate smart card reader. Applicants should notify HKPost immediately of any incorrect information of the certificate.

4.2 e-Cert (Organisational) Certificates

4.2.1 Certificate Application

4.2.1.1 Application Processing

4.2.1.1.1 Applicants for e-Cert (Organisational) certificates must complete and submit an application form, including supplementary application forms as required by the HKPost, along with the other documentation referred to in the application forms and appropriate subscription fee at a designated HKPost premises or premises of other organisations designated by HKPost.

4.2.1.1.2 For an e-Cert (Organisational) certificate without MR Status, the Applicant, at the time of application, may choose an e-Cert Storage Medium for issuance of the e-Cert and the Private Key. The Applicant may also, at the time of submitting an application form, request an additional copy of the e-Cert and the Private Key to be stored in Alternative Storage Medium that is provided by the Applicant. If HKPost considers the request acceptable, HKPost shall store the additional copy of the e-Cert and the Private Key in each of the Alternative Storage Medium. In such case, the process in Section 4.2.2 is also applicable to the additional copy of the e-Cert and the Private Key. In particular, the additional copy of the e-Cert and the Private Key will be protected by e-Cert PIN and delivered to the Applicant in a secure manner.

However, for an e-Cert (Organisational) with MR Status certificate, the Applicant, at the time of application, can only choose the designated PKCS#11 compatible e-Cert Storage Medium for issuance of the e-Cert and the Private Key.

4.2.1.1.3 HKPost has implemented internal procedures and controls over the preparation, activation, usage, distribution and termination of any key storage media. The procedures and controls are regularly reviewed by independent third party.

4.2.1.1.4 By submitting an e-Cert application form, the Applicant authorises the publication of the e-Cert to any other person or in the HKPost Repository and thus accepts the e-Cert to be issued to the Applicant.

4.2.1.2 Identity Verification

The documentation required for proving the identity of the Subscriber Organisation, Authorised Representative(s) and Authorised Users is stipulated in Section 3.1.8 of this CPS. The e-Cert PIN envelopes will be passed to the Authorised Representative in person by hand at the juncture of submission of the application at a designated HKPost premises, or delivered to the Authorised Representative in a secure manner such as by registered mail upon satisfactory completion of the identity verification process.

4.2.2 Certificate Issuance

4.2.2.1 Following the identity verification process, HKPost shall generate the e-Certs (including the associated key pairs) of the respective Authorised Users in a Trustworthy System and environment within HKPost's premises to ensure that the Private Key will not be tampered with.

4.2.2.2 The Private Key and e-Cert, which are protected by a PIN, will then be stored on the e-Cert Storage Medium and the Alternative Storage Medium, if any, selected by the Applicant. The e-Cert Storage Medium and the Alternative Storage Medium, if any, which will be sealed up in a tamper-proof envelope or other forms of containers, will then be delivered to the Authorised Representative in a secure manner such as by registered mail.

4.2.2.3 The Subscriber Organisation agrees that it is fully accountable for the safe custody of the Private Key upon receipt of the e-Cert Storage Medium and the Alternative Storage Medium, if any, and agrees that they will be responsible for any consequences under any circumstances for the compromise of the Private Key.

4.2.2.4 All Private Keys stored in the HKPost system are in an encrypted form. Proper security controls are in place to guard against unauthorised access to and disclosure of the encrypted Private Keys. Upon completion of delivery of the e-Certs and Private Keys to the Authorised Representative, the respective Private Keys will be purged from the HKPost system.

4.2.3 Publication of e-Cert

Under the Ordinance, HKPost shall publish promptly the accepted and issued e-Cert in the Repository (see Section 2.5). Applicants can either verify the information on the certificate by browsing the certificate file or through HKPost CA Repository. Applicants should notify HKPost immediately of any incorrect information of the certificate.

4.3 e-Cert (Encipherment) Certificates

4.3.1 Certificate Application

4.3.1.1 Application Processing

4.3.1.1.1 Applicants for e-Cert (Encipherment) certificates must complete and submit an application at a designated HKPost premises or premises of other organisations designated by HKPost.

4.3.1.1.2 In the application, the Applicant may choose an e-Cert Storage Medium for issuance of the e-Cert and the Private Key. The Applicant may, at the time of submitting an application form, request an additional copy of the e-Cert and the Private Key to be stored in Alternative Storage Medium that is provided by the Applicant. If HKPost considers the request acceptable, HKPost shall store the additional copy of the e-Cert and the Private Key in each of the Alternative Storage Medium. In such case, the process in section 4.3.2 is also applicable to the additional copy of the e-Cert and the Private Key. In particular, the additional copy of the e-Cert and the Private Key will be protected by e-Cert PIN and delivered to the Applicant in a secure manner.

4.3.1.1.3 By submitting an e-Cert application form, the Applicant authorises the publication of the e-Cert to any other person or in the HKPost Repository and thus accepts the e-Cert to be issued to the Applicant.

4.3.1.2 Identity Verification

The documentation required for proving the identity of the Subscriber Organisation and Authorised Representative(s) is stipulated in Section 3.1.8 of this CPS. The e-Cert PIN envelopes will be passed to the Authorised Representative in person by hand at the juncture of submission of the application at a designated HKPost premises, or delivered to the Authorised Representative in a secure manner such as by registered mail upon satisfactory completion of the identity verification process.

4.3.2 Certificate Issuance

4.3.2.1 Following the identity verification process, HKPost shall generate the e-Certs (including the associated key pairs) of the respective Authorised Units in a Trustworthy System and environment within HKPost's premises to ensure that the Private Key will not be tampered with.

4.3.2.2 The Private Key and e-Cert, which are protected by a PIN, will then be stored on the e-Cert Storage Medium and the Alternative Storage Medium, if any, selected by the Applicant. The e-Cert Storage Medium and the Alternative Storage Medium, if any, which will be sealed up in a tamper-proof envelope or other forms of containers, will then be delivered to the Authorised Representative in a secure manner such as by registered mail.

4.3.2.3 The Subscriber Organisation agree that it is fully accountable for the safe custody of the Private Key upon receipt of the e-Cert Storage Medium and the Alternative Storage Medium, if any, and agree that they will be responsible for any consequences under any circumstances for the compromise of the Private Key.

4.3.2.4 All Private Keys stored in the HKPost system are in an encrypted form. Proper security controls are in place to guard against unauthorised access to and disclosure of the encrypted Private Keys. Upon completion of delivery of the e-Certs and Private Keys to the Authorised Representative, the respective Private Keys will be purged from the HKPost system.

4.3.3 Publication of e-Cert

Under the Ordinance, HKPost shall publish promptly the accepted and issued e-Certs in the Repository (see Section 2.5). Applicants can either verify the information on the certificate by browsing the certificate file or through HKPost CA Repository. Applicants should notify HKPost immediately of any incorrect information of the certificate.

4.4 e-Cert (Server) Certificates

4.4.1 Certificate Application

4.4.1.1 Application Processing

4.4.1.1.1 Applicants for e-Cert (Server) certificates must complete and submit an application at a designated HKPost premises or premises of other organisations designated by HKPost.

4.4.1.1.2 By submitting an e-Cert application form, the Applicant authorises the publication of the e-Cert to any other person or in the HKPost Repository and thus accepts the e-Cert to be issued to the Applicant.

4.4.1.2 Identity Verification

The documentation required for proving the identity of the Subscriber Organisation and Authorised Representative(s) is stipulated in Section 3.1.8 of this CPS. The e-Cert PIN envelopes will be passed to the Authorised Representative in person by hand at the juncture of submission of the application at a designated HKPost premises, or delivered to the Authorised Representative in a secure manner such as by registered mail upon satisfactory completion of

the identity verification process. Meanwhile, HKPost will check the Certification Authority Authorisation record(s) ("CAA Record") published for the domain name(s) to be identified in the certificate. If a CAA Record exists that does not list HKPost's domain name "hongkongpost.gov.hk" as an authorised issuer domain name, the certificate application will not be proceeded. If no CAA Record exists for the domain name(s) to be identified in the certificate, HKPost considers that the applicant allows HKPost to issue certificate for the domain name(s).

4.4.1.3 Validation of Domain Authorization or Control

With respect to the validation of domain authorization responsibilities for CA that adhere to the CA / Browser Forum Baseline Requirements ("BR"), HKPost confirms that as of the date of the e-Cert (Server) certificate was issued, HKPost has validated the applicant's ownership or control of each Fully-Qualified Domain Name ("FQDN") listed in the e-Cert (Server) certificate using one or more of the following procedures:

a) Communicating directly with the Domain Name Registrant using a postal address, email, or telephone number provided by the Domain Name Registrar and obtaining a response confirming the applicant's request for validation of the FQDN (i.e. reserved in BR 3.2.2.4.2 and BR 3.2.2.4.3);
b) Communicating directly with the Domain Name Registrant using an email address created by pre-pending 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' in the local part, followed by the at-sign ("@"), followed by the Authorization Domain Name, which may be formed by pruning zero or more components from the requested FQDN (i.e. reserved in BR 3.2.2.4.4); or
c) Relying on publicly available records from the Domain Name Registrar, such as WHOIS or other DNS record information (i.e. BR 3.2.2.4.5).

4.4.2 Certificate Issuance and Publication

4.4.2.1 Following the identity verification process, HKPost shall notify the Applicant approval of an application. The certificate issuance process is as follows:

a) An applicant generates the Private Key and public key on his/her own devices.
b) The applicant generates on his/her own devices the Certificate Signing Request (CSR) containing the public key, and transmits the CSR to HKPost through a designated web page at http://www.hongkongpost.gov.hk.
c) Upon receipt of the CSR, HKPost shall verify that the applicant is in possession of the corresponding Private Key by checking the digital signature on the CSR structure containing the public key material. HKPost shall not have possession of the applicants' Private Keys.
d) Upon verifying the applicant's possession of his/her Private Key, HKPost shall generate the certificate in which the applicant's public key will be included. To support Certificate Transparency in accordance with RFC 6962, HKPost shall submit the Certificate to two or more Certificate Transparency Logs to obtain and attach the signed certificate timestamps (SCT) to the Certificate.
e) The Applicant verifies and confirms the accuracy of the information contained in the e-Cert at the designated web page at http://www.hongkongpost.gov.hk. If the Applicant rejects the e-Cert, HKPost shall revoke that e-Cert. The issued and accepted e-Cert will then be transmitted to the Applicant and published in the Repository under the Ordinance.
f) Applicants can either verify the information on the certificate by browsing the certificate file or through HKPost CA Repository. Applicants should notify

HKPost immediately of any incorrect information of the certificate.

4.5 Timeframe for Processing Certificate Applications

HKPost shall make reasonable effort to finish the certificate application during a reasonable period of time. In circumstances where the application materials submitted by the Applicant are complete and have fulfilled all the application requirements, HKPost pledges to finish the certificate application within the following time periods:

Types of certificates	**Time periods for finishing the application**
e-Cert (Personal)	Three working days
e-Cert (Personal) with MR Status	
e-Cert (Organisational)	Ten working days
e-Cert (Organisational) with MR Status	
e-Cert (Encipherment)	
e-Cert (Server)	
e-Cert (Server) with Wildcard feature or Multi-domain feature	

For the avoidance of doubt, all Saturdays, Sundays, public holidays and for all weekdays on which a tropical cyclone warning signal no. 8 (or above) or a black rainstorm warning signal is hoisted, are not working days for the purpose of this Section 4.5.

4.6 Certificate Suspension and Revocation

4.6.1 Circumstances for Suspension and Revocation

4.6.1.1 The compromise of a HKPost Private Key will result in prompt revocation of the certificates issued under that Private Key. Procedures stipulated in the HKPost key compromise plan will be exercised to facilitate rapid revocation of all Subscriber certificates in the event of compromise of the HKPost Private Keys (see Section 4.11.2).

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

4.6.1.3 Each Subscriber MUST apply to HKPost for the revocation of the certificate in accordance with the revocation procedures in this CPS immediately after the Subscriber's Private Key, or the media containing the Private Key corresponding to the Public Key contained in an e-Cert has been, or is suspected of having been, compromised (see also Section 2.1.4(h)) or any change in the Information in the certificate provided by the Subscriber.

4.6.1.4 HKPost may suspend or revoke a certificate and will notify the Subscriber by updating the certificate revocation list, or by updating the relevant OCSP response whenever applicable and by email, if a contact email address is available, of such suspension or revocation ("Notice of Revocation") in accordance with the procedures in the CPS whenever it:

a) knows or reasonably suspects that a Subscriber's Private Key has been compromised;
b) knows or reasonably suspects that any details upon a certificate are not true or have become untrue or that the certificate is otherwise unreliable;
c) determines that a certificate was not properly issued in accordance with the CPS;
d) determines that the Subscriber had failed to meet any of the obligations set out in this CPS or the Subscriber Agreement;
e) is required to do so by any regulation, or law applicable to the certificate;
f) determines that the Subscriber has failed to pay the subscription fee;
g) knows or has reasonable cause to believe that the Subscriber whose details appear on an e-Cert (Personal) certificate:
    (i) is dead or has died;
    (ii) is or has become an undischarged bankrupt or has entered into a composition or scheme of arrangement or a voluntary arrangement within the meaning of the Bankruptcy Ordinance (Cap. 6) within 5 years preceding the date of revocation; or
    (iii) has been convicted in Hong Kong or elsewhere of an offence for which it was necessary to find that the person acted fraudulently, corruptly or dishonestly or committed an offence under the Electronic Transactions Ordinance;
h) knows or has reasonable cause to believe that the Authorised User named in an e-Cert (Organisational) certificate has ceased to be a member or employee of the Subscriber Organisation;
i) knows or has reasonable cause to believe that any of the server name identified in the Subject Name or Subject Alternative Name, if any, in an e-Cert (Server) certificate is no longer owned by the Subscriber Organisation; or
j) knows or has reasonable cause to believe that the Subscriber whose details appear on an e-Cert (Organisational), e-Cert (Server) or e-Cert (Encipherment) certificate that:

    (i) the Subscriber is in liquidation, or a winding up order relating to the Subscriber has been made by any Court of competent jurisdiction;
    (ii) the Subscriber has entered into a composition or a scheme of arrangement or a voluntary arrangement within the meaning of the Bankruptcy Ordinance (Cap.6) within 5 years preceding the date of intended revocation;
    (iii) a director, officer or employee of the Subscriber has been convicted of an offence for which it was necessary to find that that person acted fraudulently, corruptly or dishonestly or committed an offence under the Electronic Transactions Ordinance;
    (iv) a receiver or administrator has been appointed over any part of the Subscriber's assets within 5 years preceding the date of revocation; or
    (v) the Subscriber's existence cannot be attested.

4.6.1.5 HKPost shall maintain strict control over and make reasonable effort to prevent errors during certificate generation (e.g. errors in downloading certificates, mismatched key pair) that will lead to certificate revocation.

4.6.2 Revocation Request Procedure

A Subscriber, or the Authorised Representative of a Subscriber Organisation, may submit a certificate revocation request to HKPost through a designated web page on the HKPost web site at http://www.hongkongpost.gov.hk, by fax, letter mail, email or in-person. Subscribers need to submit revocation request in case they fail to pay the subscription fee and refuse to accept the promotional offer in extending the subscription period.

After receiving the revocation request, HKPost shall validate the request and verify the justifications for revocation before suspending the certificate. The certificate will be revoked,

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

The information of all certificates that have been suspended or revoked, including the reason code identifying the reason for the certificate suspension and revocation, will be included in the Certificate Revocation List (see Section 7.2). For certificates that support OCSP, their certificate status with the reason code will be included in the OCSP response for each individual certificate (see Section 7.3). A certificate that is resumed from a "suspended" status will not be included in the succeeding Certificate Revocation Lists and the certificate status in the relevant OCSP response for that certificate will become good.

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

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

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

4.6.3 Service Pledge & Update of Certificate Revocation List and OCSP Responses

a) HKPost shall exercise reasonable endeavours to ensure that within 2 working days of (1) receiving a revocation request or final confirmation of revocation from the Subscriber or (2) in the absence of such a request, the decision by HKPost to suspend or revoke the certificate, the suspension or revocation is posted to the Certificate Revocation List. For all certificates with MR Status that comply with the MRCP, the processing time shall be shortened to one working day. However, a Certificate Revocation List is not immediately published in the directory for access by the public following each certificate suspension or revocation. Only when the next Certificate Revocation List is updated and published will it reflect the suspended or revoked status of the certificate. If the certificate supports OCSP, the OCSP response for that certificate will be updated at the same time when the next Certificate Revocation List is updated and published. Certificate Revocation Lists are published daily and are archived for at least 7 years.

   For the avoidance of doubt, all Saturdays, Sundays, public holidays and for all weekdays on which a tropical cyclone warning signal no. 8 (or above) or a black

rainstorm warning signal is hoisted, are not working days for the purpose of this section 4.6.3 (a).

HKPost shall exercise reasonable endeavours to notify relevant Subscribers by updating the certificate revocation list, and the relevant OCSP response and by email, if a contact email address is available, within two working days following the suspension or revocation. For all certificates that comply the MRCP, the processing time shall be shortened to one working day.

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 or Relying Parties in respect of any such transactions if, despite the foregoing of this sub-section, they do use the certificate in a transaction.

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

HKPost shall be under no liability to Relying Parties in respect of the transactions in the period between HKPost's decision to suspend or revoke a certificate (either in response to a request or otherwise) and the appearance of the suspension or revocation status on the Certificate Revocation List, or in the period between that decision to suspend or revoke a certificate and the update of the relevant OCSP response, 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. In no circumstances does the RA itself undertake a separate duty of care to Relying Parties (the RA is simply discharging HKPost's duty of care), and accordingly, even if negligent, the RA itself cannot be held liable to Relying Parties.

d) When an e-Cert is suspended or revoked, HKPost shall publish the relevant information (including the Certificate Revocation List (such as Authority Revocation List of HKPost), and the relevant OCSP responses whenever applicable) on a timely basis.

e) The Certificate Revocation List ("CRL"), Authority Revocation List ("ARL") of HKPost and the OCSP responses are updated and published in accordance with the schedule and format specified in **Appendix C**. Supplementary update of CRL is published at the HKPost web site at http://www.hongkongpost.gov.hk on ad hoc basis.

f) HKPost's policy concerning the situation where a Relying Party is temporarily unable to obtain Information on suspended or revoked certificate is stipulated in Section 2.1.6

(Relying Parties Obligations) and Section 2.2.1 (Reasonable Skill and Care) of this CPS.

4.6.4 Effect of Revocation

Revocation terminates a certificate as of the time that HKPost posts the suspension/revocation status to the Certificate Revocation List. OCSP is only provided as an alternative to the Certificate Revocation List. In the case of a suspended or revoked e-Cert (Personal) certificate embedded in Smart ID Card, the Subscriber may leave the e-Cert on the Smart ID Card or go to one of the designated Post Offices to have his e-Cert removed from the Smart ID Card.

4.7 Termination of Certificate Subscription

Under the following three conditions, certificate subscription for Subscribers will be terminated:

a) Certificates are revoked by HKPost during their validity period;

b) Requests for termination of services are received prior to the expiry of the certificates, and are accepted by HKPost;

c) Certificates or keys have not been renewed upon the expiry of the certificates.

HKPost has clearly set out the requirements for certificate subscription termination, draw up specific workflow for certificate subscription termination and properly retain the records in accordance with the Archive Retention Period specified in Section 4.9.2.

4.8 Computer Security Audit Procedures

4.8.1 Types of Events Recorded

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

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

4.8.2 Frequency of Processing Log

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

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

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

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

4.8.6 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.

4.8.7 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.

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

4.9 Records Archival

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

- System equipment configuration files;
- Results of assessments and/or review for accreditation of the equipment (if conducted);
- Certification Practice Statement and its modifications or updates;
- Contractual agreements to which HKPost is bound;
- All certificates and CRLs as issued or published, and all OCSP responses;
- Periodic event logs;
- Other data necessary for verifying archive contents;
- Documentations of the establishment and upgrading of certificate system;
- Documentations supporting certificate application, information on the approval and rejection of certificate services, and certificate subscriber agreements;
- Audit records;
- Particulars of staff, including but not limited to information on their background, employment and training; and
- Documentations of external or internal assessments.

4.9.2 Archive Retention Period
Key and certificate information as well as archival records as specified in Section 4.9.1 are securely maintained for at least 7 years. Audit trail files are maintained in the CA system as deemed appropriate by HKPost.

4.9.3 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.

4.9.4 Archive Backup Procedures
Backup copies of the archives will be created and maintained when necessary. HKPost shall verify the consistency of archival records during the archival process. During the archival period, HKPost shall verify the consistency of all accessed records through appropriate techniques or methods.

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

4.10 Key Changeover

The lifespan of the HKPost CA and e-Cert root keys and certificates created by HKPost (See **Appendix G**) for the purpose of certifying certificates issued under this CPS is no more than 20 years. HKPost CA keys and certificates will be renewed at least 3 months before their certificates expire. Upon renewal of a root key, the associated root certificate will be published in HKPost web site http://www.hongkongpost.gov.hk for public access. The original root keys will be kept for a minimum period as specified in Section 4.9.2 for verification of any signatures generated by the original root keys. HKPost shall ensure safe and smooth transition of the entire process, with a view to minimizing the adverse effects on Subscribers and Relying Parties.

4.11 Disaster Recovery and Key Compromise Plans

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

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

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

a) Sensitive material or equipment will be locked up safely in the facility;
b) Sensitive material or equipment will be removed from the facility if it is not possible to lock them up safely in the facility or if there is a risk of damage to the material or equipment, and such material or equipment will be locked up in other temporary facilities; and

c) Access control will be enforced at all entrances and exits of the facility to protect the facility from theft and unauthorised access.

4.11.2 Key Compromise Plan

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

HKPost shall promptly notify the Government Chief Information Officer and make public announcement if a HKPost Private Key for the issuance of e-Cert certificates under this CPS has been compromised. The compromise of a HKPost Private Key will result in prompt revocation of the certificates issued under that Private Key and the issuance of new and replacement certificates. HKPost shall timely and properly inform Subscribers and Relying Parties within a reasonable period of time.

4.11.3 Key Replacement

In the event of key compromise or disaster where a HKPost Private Key for the issuance of e-Cert certificates under this CPS has been compromised or corrupted and cannot be recovered, HKPost shall promptly notify the Government Chief Information Officer and make a public announcement as to which certificates have been revoked, and how the new HKPost Public Key is provided to Subscribers, and how Subscribers are issued with new certificates. In case of revocation requests for the HKPost CA root certificate, HKPost shall only proceed subject to the confirmation of the Government Chief Information Officer.

4.11.4 Damaged Computing Resources, Software and/or Data

Business continuity plan involves formal handling procedures of damaged computing resources, software and/or data. These relevant procedures shall be reviewed and drilled annually.

When computing resources, software and/or data are damaged, HKPost shall evaluate the impact of the incidents, investigate the causes and perform system recovery operations with the system backup in order to resume the normal CA operation. If, in the circumstances when computing resources, software and/or data are damaged, the HKPost Private Key for the issuance of e-Cert certificates under this CPS has been compromised or damaged, HKPost shall promptly notify the Government Chief Information Officer and make public announcement. If, in the circumstances when computing resources, software and/or data are damaged, the Subscriber's Private Key generated by HKPost on behalf of the Subscriber has been compromised or damaged, HKPost shall promptly revoke the respective certificates and issue new and replacement certificates. HKPost shall timely and properly inform Subscribers and Relying Parties within a reasonable period of time.

4.12 CA Termination

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

4.13 RA Termination

In the event that the RA is terminated under RA agreement or under CA termination (see Section 4.12) or the RA's authority to act on behalf of HKPost is withdrawn, the e-Certs applied through the RA will remain in effect in accordance with their terms and validity.

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 defined different secure areas, and employed effective physical security control measures in accordance with the requirements of different areas to ensure the physical security of such areas. Meanwhile, HKPost shall ensure that access to each physical security layer is auditable and controllable so that only authorised personnel can access each physical security layer.

The security control measures 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. Assess shall be under control and be monitored manually or by electronic means to prevent unauthorised intrusion at all times. The access control system has included the functions of check-in/check-out record and time-out alert, and such records shall be archived on a regular basis and shall be kept for 6 months.

5.1.3 Environmental controls of Computer Room
HKPost has implemented a computer room monitoring system to provide real-time monitoring for infrastructure equipments, computer room and security protection system 24 hours a day and seven days a week. The monitoring records shall be retained for 6 months for the purposes of fault diagnosis and post-event auditing.

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

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

5.1.6 Fire and Flooding Prevention and Protection
A fire prevention plan and a fire suppression system have been established for the CA facility. Fire protective measures have complied with the requirements specified by Fire Services Department of Hong Kong. The computer room has been installed with automatic fire alarm system and fire extinguishing system. Two types of fire detectors have been installed for detecting temperature and smoke. The fire alarm system and the fire extinguishing system have been linked together. HKPost CA has also established handling procedures to protect the systems from damages or other adverse consequences arising from flooding or water leakage.

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

5.1.8 Off-site Backup
HKPost has established backup systems for critical systems (including HKPost CA System) and data (including any sensitive information and audit data). Off-site backup measures have been implemented for critical systems and data to ensure these systems and data are stored in secure facilities against theft, damage and media storage deterioration (see Section 4.11.1).

5.1.9 Protection of Paper Documents
Paper documents including Subscriber Agreements and photocopies of identity confirmation documents are maintained by HKPost, the Contractor or its RAs in a secure fashion. Only authorised personnel are permitted access to the paper records.

5.1.10 Waste Disposal Procedures
HKPost shall strictly handle any wastes containing privacy or sensitive information and ensure thorough physical destruction of such wastes or complete deletion of data stored in such wastes to prevent unauthorised access to, use or disclosure of privacy or sensitive information stored in such wastes.

5.2 Procedural Controls

5.2.1 Trusted Role
Employees, contractors, and consultants of HKPost, of the Contractor and of RAs acting on behalf of HKPost (collectively "Personnel") that have access to or control of cryptographic or other operations that may materially affect the issuance, use, or revocation of certificates, including access to restricted operations of HKPost's CA database, are considered to be serving in a trusted role. Such Personnel include, but are not limited to, system administration personnel, operators, engineering personnel, and executives who are assigned to oversee HKPost's CA operation. Based on the nature of operations as well as the rights for their positions, the personnel working in trusted positions shall be granted with the rights to access systems and physical environments, and shall adopt appropriate access control techniques to maintain a complete record of all sensitive operations performed by such personnel.

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

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

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

5.3 Personnel Controls

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

5.3.2 Background Investigation

HKPost conducts and/or requires the Contractor and RAs to conduct investigations of personnel who serve in trusted roles (prior to their employment and periodically thereafter as necessary and require the personnel to present their valid proof of identity) to verify such 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. Also, relevant security provisions have been incorporated in staff contract and the personnel must agree and sign the contract before their employment.

5.3.3 Training Requirements

HKPost, the Contractor or its RAs shall ensure all their staff (including those assuming the trusted roles) to possess the required technical qualifications and expertise so that they can effectively carry out their duties and responsibilities. At the same time, they shall provide appropriate and sufficient training for their staff (at least once a year for those holding core positions) to ensure their capabilities in carrying their duties as well as effective implementation and compliance with security policies. The content of training may include but not limited to:

a) Appropriate technical training;
b) Rules, mechanisms and procedures;
c) Procedures for handling security incidents and notifying senior management of major security incidents.

5.3.4 Assessment of Existing Staff

HKPost, the Contractor or its RAs shall formulate appropriate control measures to assess the performance of their staff. For example:

a) Performance assessment on regular basis;
b) Formal disciplinary procedures (including procedures for handling unauthorised activities);
c) Formal procedures for service termination.

5.3.5 Documentation Supplied To Personnel

HKPost personnel and those of the Contractor's and RA's receive comprehensive user manuals detailing the procedures for certificate creation, issuance, updating, renewal, and revocation, and other software functionality relative to their role.

6. TECHNICAL SECURITY CONTROLS

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

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Key pairs for HKPost and Applicants/Subscribers are generated through a procedure such that the Private Key cannot be accessed by anyone other than the authorised user of the Private Key unless there is some compromise of the procedure by the authorised user. HKPost generates the root key pairs for issuing certificates that conform to this CPS. In case of central key generation by HKPost on behalf of the Applicants, the Applicants' Private Keys will be purged from the HKPost system upon completion of delivery of the e-Certs and Private Keys to the Applicants.

6.1.2 Subscriber Public Key Delivery

Key pairs for e-Cert (Personal), e-Cert (Organisational) and e-Cert (Encipherment) certificates will be generated under the central key generation by HKPost on behalf of the Applicant/Subscriber. In respect of e-Cert (Server), the Applicant's Public Key which will be generated by the Applicant must be transferred to HKPost using a method designed to ensure that :

- The Public Key is not changed during transit; and
- The sender possesses the Private Key that corresponds to the transferred Public Key.

6.1.3 Public Key Delivery to Subscriber

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

6.1.4 Key Sizes

The HKPost signing key pair is 2048-bit RSA. Subscriber key pair is 2048-bit RSA.

6.1.5 Standards for Cryptographic Module

Signing key generation, storage, and signing operations performed by HKPost are conducted within a hardware cryptographic module.

6.1.6 Key Usage Purposes

Keys used in e-Cert (Personal), e-Cert (Organisational) and e-Cert (Encipherment) certificates may be used for Digital Signatures and conducting enciphered electronic communications. Keys used in e-Cert (Server) certificates are used for the purposes of conducting enciphered electronic communications and server authentication only. If digital signature Key Usage is enabled in the e-Cert (Server) certificates (referred to in **Appendix B**), the digital signatures supported by the e-Cert (Server) certificates are to be used only for server authentication and for establishment of secure communication channels with the server. HKPost Root Key (the key used to create or issue certificates that conform to this CPS) is used only for signing (a) certificates, (b) Certificate Revocation Lists and (c) OCSP signer's certificates.

6.2 Private Key Protection

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

6.2.2 Private Key Multi-Person Control
HKPost Private Keys are stored in tamper-proof hardware cryptographic devices. HKPost implements multi-person control (2 out of 3 multi-person control) over the activation, usage, deactivation of HKPost Private Keys.

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

6.2.4 Backup of HKPost Private Keys
Each HKPost Private Key is backed up by encrypting and storing it in devices which conform to FIPS 140-1 Level 2 security standard. Backup of the HKPost Private Key is performed in a manner that requires more than one person to complete. The backup Private Keys must be activated by more than one person. No other Private Keys are backed-up. All Private Keys will not be archived.

6.2.5 Private Key Transfer between Cryptographic Modules
When the HKPost Private Keys are transferred from one hardware cryptographic module to another, the Private Key will be transferred in encrypted form between the modules, and mutual authentication between the modules will be performed prior to the transfer. In addition, HKPost has implemented strict key management processes for controls of Private Keys transfer in order to protect the HKPost Private Keys from being lost, stolen, tampered, disclosed or used without authorization.

6.3 Other Aspects of Key Pair Management

HKPost CA root keys will be used for no more than 20 years (see also Section 4.10). All HKPost key generation, key destruction, key storage, certificate revocation list signing operations, and OCSP signing operations are performed in a hardware cryptographic module. Archival of HKPost Public Keys is performed as specified in Section 4.9.

6.4 Computer Security Controls

HKPost implements multi-person control over the life cycle of activation data such as PINs and passwords for accessing the CA systems. Security procedures are in place to prevent and detect unauthorised access, modification, or compromise of the CA systems, in order to ensure the security and reliability of the CA systems which are hosting software, data and documents. With these procedures, the CA systems are protected from unauthorised internal or external access. Such security controls are subject to compliance assessment as specified in Section 2.6. HKPost implements stringent management mechanism to control and monitor the operating systems, in order to prevent unauthorised modification. When processing disposal of waste devices, HKPost will exercise reasonable endeavours to erase their storage with confirmation for which may contain information related to the security of e-Cert service.

6.5 Life Cycle Technical Security Controls

HKPost implements controls over the procedures for the procurement and development of software and hardware for HKPost CA systems. Change control procedures are in place to control and monitor all revisions and enhancements to be made to the components of such systems. These procedures and controls shall include but not limited to:

a) Adoption of a set of uniform and effective internal standards for system development, whether it is conducted by the staff of HKPost or other parties;
b) Effective procedures for segregation of production and development environments;
c) Effective procedures for segregation of duties between operational, maintenance and development personnel;
d) Effective access controls over access to data and systems held in the production and development environments;
e) Effective controls (including but not limited to version control, stringent testing and verification) over change control process (including but not limited to normal and emergency changes to systems and data);
f) Procedures for conducting security checking and assessment on systems before going online to see whether there are security vulnerabilities or intrusion risks;
g) Effective procedures for the proper management of the acquisition of equipment and services; and
h) At least three trusted personnel required to participate in the access to HKPost's hardware cryptographic devices throughout their lifecycle (from the commissioning of these devices to their logical/physical destruction).

6.6 Network Security Controls

HKPost shall implement security measures such as multi-level firewall, intrusion detection system, security audit, anti-virus system to protect the HKPost's network environment. Timely version update, regular risk assessment and audit for network environment shall be conducted in order to detect intrusion risks and minimize risks from the network.

6.7 Cryptographic Module Engineering Controls

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

7. CERTIFICATE, CERTIFICATE REVOCATION LIST AND ONLINE CERTIFICATE STATUS PROTOCOL RESPONSE PROFILES

7.1 Certificate Profile

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

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

7.2 Certificate Revocation List Profile

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

7.3 Online Certificate Status Protocol Response Profile

The HKPost Online Certificate Status Protocol response conforms to RFC6960 and RFC5019 (see **Appendix C**).

8. CPS ADMINISTRATION

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

Appendix A - Glossary

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

"Accept", in relation to a certificate

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

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

"Alternative Storage Medium" means a storage medium provided by the Applicant, such as floppy disk, recordable CD, USB flash drive or PKCS#11 compliant device, which holds an additional copy of the e-Cert and the Private Key.

"Applicant" means a natural or legal person who has applied for an e-Cert.

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

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

"Authorised Unit" means a unit of a Subscriber Organisation whom that Subscriber Organisation has duly authorised to use the Private Key of a HKPost e-Cert (Encipherment) issued to that Subscriber Organisation.

"Authorised User" means a member or employee of a Subscriber Organisation whom that Subscriber Organisation has duly authorised the use of the Private Key of an e-Cert (Organisational) issued to that Subscriber Organisation. Member refers to a person with whom the Subscriber Organisation has maintained any forms of lawful legal relations.

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

"CA / Browser Forum Baseline Requirements" means the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, published at https://cabforum.org.

"CA" means Certification Authority.

"CAA Record" means a Certification Authority Authorisation DNS Resource Record that allows a DNS domain name holder to specify the Certification Authorities (CAs) authorised to issue certificates for that domain.

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

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

"Certificate Transparency" means according to the requirement of RFC 6962 and Google, a publicly auditable and monitoring log of server certificates issued by Certificate Authority (CA).

"Certificate Transparency Log" is a simple network services that maintain cryptographically assured, publicly auditable, append-only records of server certificates.

"Contract" means the outsourcing contract that HKPost has awarded to the Contractor for operating and maintaining the systems and services of the HKPost CA as stipulated in this CPS on behalf of HKPost for a period from 1 April 2012 to 31 March 2018.

"Contractor" means Certizen Limited, together with its Subcontractor(s), if any as listed in **Appendix F**, being an agent of HKPost CA appointed pursuant to Section 3.2 of the COP for operating and maintaining the systems and services of the HKPost CA in accordance with the terms of the Contract.

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

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

"CPS" means Certification Practice Statement.

"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.

"Domain Name Registrant" means person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a domain name is used.

"Domain Name Registrar" means a person or entity that registers domain names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national domain name authority/registry, or (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assigns).

"e-Cert File Card" means a smart card which is an e-Cert Storage Medium.

"e-Cert File USB" means a USB flash drive which is an e-Cert Storage Medium. The prevailing cost of an e-Cert File USB is published at HKPost web site at http://www.hongkongpost.gov.hk.

"e-Cert Storage Medium" means a storage medium, such as e-Cert File Card or e-Cert File USB, for storage of the e-Cert and the Private Key.

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

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

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

"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.

"IRD Reference Number" means a number being assigned by the Inland Revenue Department to a Reporting Financial Institution as referred in the Inland Revenue Ordinance

(Cap. 112). The IRD Reference Number will be given in a certification letter issued to the Reporting Financial Institution issued by Inland Revenue Department.

"Issue" in relation to a certificate, means to:

(a) create the certificate, and then notify the person named or identified in the certificate as the person to whom the certificate is issued of the information on the person as contained in the certificate; or

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

"Key Pair", in an Asymmetric 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.

"Mutual Recognition Certificate Policy" or **"MRCP"** means the Certificate Policy for Mutual Recognition of Electronic Signature Certificates issued by Hong Kong and Guangdong under the Arrangement for Mutual Recognition of Electronic Signature Certificates issued by Hong Kong and Guangdong.

"Multi-domain feature" in relation to a HKPost e-Cert (Server) certificate, means a feature that enables the use of the certificate for multiple server names by specifying the server names in the Subject Alternative Name extension of the certificate.

"Mutual Recognition Status" or **"MR Status"** in relation to a HKPost e-Cert (Personal) or HKPost e-Cert (Organisational), means a certificate that complies with the Certificate Policy for Mutual Recognition of Electronic Signature Certificates Issued by Hong Kong and Guangdong ("MRCP") issued by the governments of Hong Kong and Guangdong for cross-boundary use between the two places.

"OCSP" means Online Certificate Status Protocol.

"Online Certificate Status Protocol" means an online certificate checking protocol that enables Relying Party to determine the status of e-Cert.

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

"PIN" means a secret password protecting the corresponding Private Key and e-Cert of respective Subscriber.

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

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

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

"Private Key" means the key of a Key Pair used to generate a Digital Signature.

"Public Key" means the key of a Key Pair used to verify a Digital Signature.

"RA" means Registration Authority.

"Recognized CA" means Recognized Certification Authority.

"Recognized Certificate" means

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

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

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

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

"Relying Party" means the recipient of a certificate who relies on the certificate and/or the electronic signature verified by the certificate.

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

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

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

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

"Signed Certificate Timestamp" means when a valid server certificate is submitted to a Certificate Transparency Log, the log responds with a signed certificate timestamp (SCT), which is simply a promise to add the certificate to the log within some time period.

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

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

"Subcontractor" means an organisation that has been appointed by Certizen Limited for the performance of part of the Contract.

"Subscriber" means a person who:

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

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

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

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

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

"Wildcard feature" in relation to an e-Cert (Server) certificate, means a feature that enables the use of the certificate for all server names at the same domain or sub-domain level owned by the Subscriber Organisation by specifying a wildcard character (i.e. an asterisk character '*') in the left-most component of the fully qualified domain name of the server name contained in the certificate.

"Subject Name" means the information of the name of certificate holder.

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

This appendix provides the formats of e-Cert issued by the Sub CAs "Hongkong Post e-Cert CA 1 - 10", "Hongkong Post e-Cert CA 1 - 14" and "Hongkong Post e-Cert CA 1 - 15" under this CPS. For the format of e-Cert issued by the other Sub CA(s) of HKPost or issued under other CPS, please refer to the prevailing CPS in respect of the issuance date of the e-Cert or the OID as specified in the "Certificate Policies" of the e-Cert concerned.

1) e-Cert (Personal) Certificate Format

Field Name		**Field Content**		
		Hongkong Post e-Cert (Personal) certificates	**HongKong Post e-Cert (Personal) with MR Status certificates**	**Hongkong Post e-Cert (Personal) certificates issued to persons aged under 18**
Standard fields				
Version		X.509 v3		
Serial number		[3-byte hexadecimal number set by HKPost CA system]		
Signature algorithm ID		sha1RSA		
Issuer name		cn=Hongkong Post e-Cert CA 1 – 10 o=Hongkong Post c=HK		
Validity period	**Not before**	[UTC time set by HKPost CA system]		
	Not after	[UTC time set by HKPost CA system]		
Subject name		cn=[HKID name] (Note 1) e=[email address] (Note 2) ou=[SRN] (Note 3) o=Hongkong Post e-Cert (Personal) c=HK		cn=[HKID name] (Note 1) e=[email address] (Note 2) ou=[SRN] (Note 3) o=Hongkong Post e-Cert (Personal/Minor) (Note 4) c=HK
Subject public key info		Algorithm ID: RSA Public Key: 2048-bit key size		
Issuer unique identifier		Not used		
Subject unique identifier		Not used		
Standard extension (Note 5)				
Authority key identifier	**Issuer**	cn=Hongkong Post Root CA 1 o=Hongkong Post c=HK		
	Serial number	[Inherited from Issuer]		
Key usage		Non-repudiation, Digital Signature, Key Encipherment **(This field will be set Critical.)**	Non-repudiation, Digital Signature **(This field will be set Critical.)**	Non-repudiation, Digital Signature, Key Encipherment **(This field will be set Critical.)**
Certificate policies		Policy Identifier = [OID] (Note 6) Policy Qualifier Id = CPS Qualifier = [URL of CPS]	Policy Identifier =[OID](Note 6) Policy Qualifier Id = CPS Qualifier : [URL of CPS] Policy Identifier =2.16.344.8.2.2008.810.2.2012.1.0(Note 7) Policy Qualifier Id = CPS Qualifier = [URL of CPS] Policy Identifier =	Policy Identifier = [OID] (Note 6) Policy Qualifier Id = CPS Qualifier = [URL of CPS]

			1.3.6.1.4.1.16030.1.4(Note8) Policy Qualifier Id = CPS Qualifier = [URL of CPS]	
Subject alternative name	**DNS**	encrypted(HKID) (Note 9)		
	rfc822	[Applicant's email address] (Note 2)		
Issuer alternative name		Not used		
Basic constraints	**Subject type**	End Entity		
	Path length constraint	None		
Extended key usage		Not used		
CRL distribution points		Distribution Point Name = [URL of CRL Distribution Point] (Note 10)		
Netscape extension (Note 5)				
Netscape cert type		SSL Client, S/MIME		
Netscape SSL server name		Not used		
Netscape comment		Not used		

Note

1. Applicant name format: Surname (in capital) + Given name (e.g. CHAN Tai Man David).
2. Email address provided by Applicant (blank if null). That email address has not been verified.
3. SRN: 10-digit Subscriber Reference Number
4. "e-Cert (Personal/Minor)" indicates that the Applicant is under 18 at the time the e-Cert is issued (see Section 3.1.1.2 of this CPS).
5. All standard extensions and Netscape extensions are set as "non-critical" unless otherwise specified.
6. The OID of this CPS is included in this field. Please refer to Section 1.1 of this CPS for the OID of this CPS.
7. The OID of the MRCP is included in this field for identification of the certificate which is issued in compliance with MRCP.
8. The OID for supporting Adobe PDF signing is included in this field.
9. The Applicant's HKID number (**hkid_number** - including the check digit) will be stored in the certificate in the form of a hash value of the HKID number (**cert_hkid_hash**) which has been signed by the Private Key of the Applicant:

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

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

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

10. URL of CRL Distribution Point is http://crl1.hongkongpost.gov.hk/crl/eCertCA1-10CRL1_<xxxxx>.crl which are partitioned CRLs issued by the Sub CA "Hongkong Post e-Cert CA 1 - 10", where <xxxxx> is a string of five alphanumeric characters generated by the CA system. HKPost CA publishes a number of partitioned CRLs. If a certificate is suspended or revoked, its information will be published in the partitioned CRL at the URL specified in this CRL Distribution Point field.

2) e-Cert (Organisational) Certificate Format

Field Name		Field Content	
		e-Cert (Organisational) certificates	**e-Cert (Organisational) with MR Status certificates**
Standard fields			
Version		X.509 v3	
Serial number		[3-byte hexadecimal number set by HKPost CA system]	
Signature algorithm ID		sha1RSA	
Issuer name		cn=Hongkong Post e-Cert CA 1 - 10 o=Hongkong Post c=HK	
Validity period	**Not before**	[UTC time set by HKPost CA system]	
	Not after	[UTC time set by HKPost CA system]	
Subject name		cn=[Authorised User's name] (Note 1) e=[email address] (Note 2) ou=[SRN] (Note 3) ou=[(BRN or IRD Reference Number)+CI/CR+Others] (Note 4) ou=[Subscriber Organisation Name] (Note 5) ou=[Subscriber Organisation branch/dept] (Note 5) o=Hongkong Post e-Cert (Organisational) c=HK	
Subject public key info		Algorithm ID: RSA Public Key: 2048-bit key size	
Issuer unique identifier		Not used	
Subject unique identifier		Not used	
Standard extension (Note 6)			
Authority key identifier	**Issuer**	cn=Hongkong Post Root CA 1 o=Hongkong Post c=HK	
	Serial number	[Inherited from Issuer]	
Key usage		Non-repudiation, Digital Signature, Key Encipherment **(This field will be set Critical.)**	Non-repudiation, Digital Signature **(This field will be set Critical.)**
Certificate policies		Policy Identifier = [OID] (Note 7) Policy Qualifier Id = CPS Qualifier = [URL of CPS]	Policy Identifier =[OID] (Note 7) Policy Qualifier Id = CPS Qualifier : [URL of CPS] Policy Identifier =2.16.344.8.2.2008.810.2.2012.1.0(Note 8) Policy Qualifier Id = CPS Qualifier = [URL of CPS] Policy Identifier = 1.3.6.1.4.1.16030.1.4(Note 9) Policy Qualifier Id = CPS Qualifier = [URL of CPS]
Subject alternative name	**DNS**	[0 to 10 application-specific code(s)] (Note 10)	
	First Directory Name	ou=[Subscriber Organisation's Chinese name] (Note 5) ou=[Subscriber Organisation's Chinese branch/dept name] (Note 5)	
	rfc822	[email address] (Note 2)	
Issuer alternative name		Not used	
Basic constraints	**Subject type**	End Entity	
	Path length constraint	None	
Extended key usage		SSL Client, S/MIME	
CRL distribution points		Distribution Point Name = [URL of CRL Distribution Point] (Note 11)	
Netscape extension (Note 6)			
Netscape cert type		SSL Client, S/MIME	

Field Name		Field Content	
		e-Cert (Organisational) certificates	e-Cert (Organisational) with MR Status certificates
Netscape SSL server name		Not used	
Netscape comment		Not used	

Note

1. Authorised User name format: Surname (in capital) + Given name (e.g. CHAN Tai Man David).
2. Email address provided by Authorised User (blank if null). That email address has not been verified.
3. SRN: 10-digit Subscriber Reference Number
4. Business Registration Certificate Number (BRN): a string of 16 digits/alphabets [filled with all zeroes if BRN is not available]. Alternatively for organisations who present a copy of certification letter issued by the Inland Revenue Department in place of a copy of Business Registration Certificate, the IRD Reference Number of the certification letter, which is a string of 8 digits/alphabets, together with 8 trailing zeros, is included in BRN field. Certificate of Incorporation (CI)/ Certificate of Registration (CR): a string of 8 digits/alphabets [filled with leading zeros if CI/CR is shorter than 8 digits/alphabets, or all zeroes if CI/CR is not available]. Others: a string of max. 30 digits/alphabets (blank if null). For HKSAR government departments, BRN and CI/CR are filled with zeroes, department name in abbreviation (e.g. HKPO for Hongkong Post) is placed in Others.
5. For organisations who subscribe to e-Cert and are companies with company names in the Chinese language only, a default name "***CHINESE NAME ONLY***" will be set for the company's English name. In all circumstances when the company's Chinese name is provided and verified by HKPCA, it will be included in the First Directory Name of the Subject Alternative Name field (see Section 3.1.1.7 of this CPS). Chinese name must adopt the international coding standard ISO/IEC 10646.
6. All standard extensions and Netscape extensions are set as "non-critical" unless otherwise specified.
7. The OID of this CPS is included in this field. Please refer to Section 1.1 of this CPS for the OID of this CPS.
8. The OID of the MRCP is added in this field for identification of the certificate which is issued in compliance with MRCP.
9. The OID for supporting Adobe PDF signing is added in this field.
10. The application-specific code for particular application is defined in this field (see **Appendix H**).
11. URL of CRL Distribution Point is http://crl1.hongkongpost.gov.hk/crl/eCertCA1-10CRL2.crl which is a partitioned CRL issued by the Sub CA "Hongkong Post e-Cert CA 1 - 10".

3) e-Cert (Encipherment) Certificate Format

Field Name		Field Content
Standard fields		
Version		X.509 v3
Serial number		[3-byte hexadecimal number set by HKPost CA system]
Signature algorithm ID		sha1RSA
Issuer name		cn=Hongkong Post e-Cert CA 1 - 10 o=Hongkong Post c=HK
Validity period	**Not before**	[UTC time set by HKPost CA system]
	Not after	[UTC time set by HKPost CA system]
Subject name		cn=[Authorised Unit name] (Note 1) e=[email address] (Note 2) ou=[SRN] (Note 3) ou=[BRN+CI/CR+Others] (Note 4) ou=[Subscriber Organisation Name] (Note 5) ou=[Subscriber Organisation branch/dept] o=Hongkong Post e-Cert (Encipherment) c=HK
Subject public key info		Algorithm ID: RSA Public Key: 2048-bit key size
Issuer unique identifier		Not used
Subject unique identifier		Not used
Standard extension (Note 6)		
Authority key identifier	**Issuer**	cn=Hongkong Post Root CA 1 o=Hongkong Post c=HK
	Serial number	[Inherited from Issuer]
Key usage		Digital Signature, Key Encipherment **(This field will be set Critical.)**
Certificate policies		Policy Identifier = [OID] (Note 7) Policy Qualifier Id = CPS Qualifier = [URL of CPS]
Subject alternative name	**DNS**	Not used
	Rfc822	[email address] (Note 2)
Issuer alternative name		Not used
Basic constraints	**Subject type**	End Entity
	Path length constraint	None
Extended key usage		Not used
CRL distribution points		Distribution Point Name = [URL of CRL Distribution Point] (Note 8)
Netscape extension (Note 6)		
Netscape cert type		SSL Client, S/MIME
Netscape SSL server name		Not used
Netscape comment		This e-Cert is used ONLY (i) to send encrypted electronic messages to the Subscriber Organisation; (ii) to permit the Subscriber Organisation to decrypt messages; and (iii) to permit the Subscriber Organisation to acknowledge receipt of the encrypted message by sending an acknowledgement with a digital signature added to it to confirm the identity of the receiving Subscriber Organisation. For terms and conditions governing the use of this e-Cert, please see the e-Cert CPS which can be viewed at http://www.hongkongpost.gov.hk.

Note

1. Name of the Authorised Unit of the Subscriber Organisation.

2. Email address provided by the Authorised Representative

3. SRN: 10-digit Subscriber Reference Number

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

5. For organisations who subscribe to e-Cert and are companies with company names in the Chinese language only or who have provided their company's Chinese name only, their company names will not be included in this field (see Section 3.1.1.7 of this CPS).

6. All standard extensions and Netscape extensions are set as “non-critical” unless otherwise specified.

7. The OID of this CPS is included in this field. Please refer to Section 1.1 of this CPS for the OID of this CPS.

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

4) e-Cert (Server) Certificate Format

For e-Cert (Server) issued by Sub CA "Hongkong Post e-Cert CA 1 - 10" using SHA-1 hash algorithm (without OCSP support):-

Field Name		**Field Content**		
		Hongkong Post e-Cert (Server) certificates	**Hongkong Post e-Cert (Server) with Wildcard feature certificates**	**Hongkong Post e-Cert (Server) with Multi-domain feature certificates**
Standard fields				
Version		X.509 v3		
Serial number		[3-byte hexadecimal number set by HKPost CA system]		
Signature algorithm ID		sha1RSA		
Issuer name		cn=Hongkong Post e-Cert CA 1 - 10 o=Hongkong Post c=HK		
Validity period	**Not before**	[UTC time set by HKPost CA system]		
	Not after	[UTC time set by HKPost CA system]		
Subject name		cn=[Server Name] (Note 1) ou=[SRN] (Note 2) ou=[BRN+CI/CR+Others] (Note 3) ou=[Subscriber Organisation Name] (Note 4) ou=[Subscriber Organisation branch/dept] o=Hongkong Post e-Cert (Server) c=HK		
Subject public key info		Algorithm ID: RSA Public Key: 2048-bit key size		
Issuer unique identifier		Not used		
Subject unique identifier		Not used		
Standard extension (Note 5)				
Authority key identifier	**Issuer**	cn=Hongkong Post Root CA 1 o=Hongkong Post c=HK		
	Serial number	[Inherited from Issuer]		
Key usage		Key Encipherment	Digital Signature and Key Encipherment	
		(This field will be set Critical.)		
Certificate policies		Policy Identifier = [OID] (Note 6) Policy Qualifier Id = CPS Qualifier = [URL of CPS]		
Subject alternative name	**DNS**	Not used	[Server Name in Subject name field] + [Server Name without wildcard component] (Note 7)	[Server Name in Subject name field] + [0 to 49 Additional Server Name(s)] (Note 8)
	rfc822	Not used		
Issuer alternative name		Not used		
Basic constraints	**Subject type**	End Entity		
	Path length constraint	None		
Extended key usage		Not used	Server Authentication Client Authentication	
CRL distribution points		Distribution Point Name = [URL of CRL Distribution Point] (Note 9)		
Netscape extension (Note 5)				
Netscape cert type		SSL Server	Not used	
Netscape SSL server name		Not used		

Field Name		Field Content		
		Hongkong Post e-Cert (Server) certificates	**Hongkong Post e-Cert (Server) with Wildcard feature certificates**	**Hongkong Post e-Cert (Server) with Multi-domain feature certificates**
Netscape comment		Not used		

For e-Cert (Server) issued by Sub CA "Hongkong Post e-Cert CA 1 - 14" using SHA-256 hash algorithm (without OCSP support):-

Field Name		Field Content		
		Hongkong Post e-Cert (Server)	**Hongkong Post e-Cert (Server) with Wildcard feature**	**Hongkong Post e-Cert (Server) with Multi-domain feature**
Standard fields				
Version		X.509 v3		
Serial number		[20-byte hexadecimal number set by HKPost CA system]		
Signature algorithm ID		sha256RSA		
Issuer name		cn=Hongkong Post e-Cert CA 1 - 14 o=Hongkong Post c=HK		
Validity period	**Not before**	[UTC time set by HKPost CA system]		
	Not after	[UTC time set by HKPost CA system]		
Subject name		cn=[Server Name] (Note 1) ou=[SRN] (Note 2) ou=[BRN+CI/CR+Others] (Note 3) ou=[Subscriber Organisation Name] (Note 4) ou=[Subscriber Organisation branch/dept] o=Hongkong Post e-Cert (Server) c=HK		
Subject public key info		Algorithm ID: RSA Public Key: 2048-bit key size		
Issuer unique identifier		Not used		
Subject unique identifier		Not used		
Standard extension (Note 5)				
Authority Information Access	**Certification Authority Issuer**	[URL of the Issuer's public certificate]		
Authority key identifier		[Subject Key Identifier of the issuer's certificate]		
Subject Key Identifier		[hash value of the Subject's public key]		
Key usage		Key Encipherment	Digital Signature and Key Encipherment	
		(This field will be set Critical.)		
Certificate policies		Policy Identifier = [OID] (Note 6) Policy Qualifier Id = CPS Qualifier = [URL of CPS]		
Subject alternative name	**DNS**	Not used	[Server Name in Subject name field] + [Server Name without wildcard component] (Note 7)	[Server Name in Subject name field] + [0 to 49 Additional Server Name(s)] (Note 8)
	rfc822	Not used		
Issuer alternative name		Not used		
Basic constraints	**Subject type**	End Entity		

Field Name		Field Content		
		Hongkong Post e-Cert (Server)	**Hongkong Post e-Cert (Server) with Wildcard feature**	**Hongkong Post e-Cert (Server) with Multi-domain feature**
	Path length constraint	None		
Extended key usage		Not used	Server Authentication Client Authentication	
CRL distribution points		Distribution Point Name = [URL of CRL Distribution Point] (Note 10)		
Netscape extension (Note 5)				
Netscape cert type		SSL Server	Not used	
Netscape SSL server name		Not used		
Netscape comment		Not used		

For e-Cert (Server) issued by Sub CA "Hongkong Post e-Cert CA 1 - 15" using SHA-256 hash algorithm (with OCSP support):-

Field Name		Field Content		
		Hongkong Post e-Cert (Server)	**Hongkong Post e-Cert (Server) with Wildcard feature**	**Hongkong Post e-Cert (Server) with Multi-domain feature**
Standard fields				
Version		X.509 v3		
Serial number		[20-byte hexadecimal number set by HKPost CA system]		
Signature algorithm ID		sha256RSA		
Issuer name		cn=Hongkong Post e-Cert CA 1 - 15 o=Hongkong Post l=Hong Kong s=Hong Kong c=HK		
Validity period	**Not before**	[UTC time set by HKPost CA system]		
	Not after	[UTC time set by HKPost CA system]		
Subject name		cn=[Server Name] (Note 1) ou=[SRN] (Note 2) ou=[BRN+CI/CR+Others] (Note 3) ou=Hongkong Post e-Cert (Server) ou=[Subscriber Organisation branch/dept] o=[Subscriber Organisation Name] (Note 4) l=Hong Kong s=Hong Kong c=HK		
Subject public key info		Algorithm ID: RSA Public Key: 2048-bit key size		
Issuer unique identifier		Not used		
Subject unique identifier		Not used		
Standard extension (Note 5)				
Authority Information Access	**Certification Authority Issuer**	[URL of the Issuer's public certificate]		
	OCSP	[URL of the OCSP Responder] (Note 12)		
Authority key identifier		[Subject Key Identifier of the issuer's certificate]		
Subject Key Identifier		[hash value of the Subject's public key]		

Field Name		Field Content		
		Hongkong Post e-Cert (Server)	**Hongkong Post e-Cert (Server) with Wildcard feature**	**Hongkong Post e-Cert (Server) with Multi-domain feature**
Key usage		Digital Signature and Key Encipherment **(This field will be set Critical.)**		
Certificate policies		Policy Identifier = [OID] (Note 6) Policy Qualifier Id = CPS Qualifier = [URL of CPS]		
Subject alternative name	**DNS**	[Server Name in Subject name field]	[Server Name in Subject name field] + [Server Name without wildcard component] (Note 7)	[Server Name in Subject name field] + [0 to 49 Additional Server Name(s)] (Note 8)
	rfc822	Not used		
Issuer alternative name		Not used		
Basic constraints	**Subject type**	End Entity		
	Path length constraint	None		
Extended key usage		Server Authentication Client Authentication		
CRL distribution points		Distribution Point Name = [URL of CRL Distribution Point] (Note 11)		
1.3.6.1.4.1.11129.2.4.2		Signed Certificate Timestamp		
Netscape extension (Note 5)				
Netscape cert type		Not used		
Netscape SSL server name		Not used		
Netscape comment		Not used		

Note

1. The server name (including the domain name of the server) owned by the Subscriber Organisation. For e-Cert (Server) with Wildcard feature, the left-most component of the fully qualified domain name of the server name must be a wildcard character (i.e. an asterisk character '*', the wildcard component), meaning that the certificate may be used for all server names at the same domain or sub-domain level owned by the Subscriber Organisation (e.g. *.hongkongpost.gov.hk, *.subdomain.hongkongpost.gov.hk).

2. SRN: 10-digit Subscriber Reference Number

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

4. For organisations who subscribe to e-Cert and are companies with company names in the Chinese language only or who have provided their company's Chinese name only, their company names will not be included in this field (see Section 3.1.1.7 of this CPS).

5. All standard extensions and Netscape extensions are set as "non-critical" unless otherwise specified.

6. The OID of this CPS is included in this field. Please refer to Section 1.1 of this CPS for the OID of this CPS.

7. Subject alternative name field of an e-Cert (Server) with Wildcard feature contains two server name entries. One entry is the Server Name as shown in the Subject name field that has the wildcard character (i.e. an asterisk character '*', the wildcard component) in the left-most component of the fully qualified domain name of the server name, and the other entry is the server name without the wildcard component (e.g. *.hongkongpost.gov.hk and hongkongpost.gov.hk).

8. Subject alternative name field of an e-Cert (Server) with Multi-domain feature may contain maximum 50 server name entries. The first entry is the Server Name as shown in the Subject name field, and there may be 0 to 49 server name entries of additional server names. No wildcard character (i.e. an asterisk character '*') will be allowed as part of any server name(s).

9. URL of CRL Distribution Point for certificates issued by Sub CA "Hongkong Post e-Cert CA 1 - 10" is:

   http://crl1.hongkongpost.gov.hk/crl/eCertCA1-10CRL1.crl which is a full CRL issued by the Sub CA "Hongkong Post e-Cert CA 1 - 10".

10. URL of CRL Distribution Point for certificates issued by Sub CA "Hongkong Post e-Cert CA 1 - 14" is:

    http://crl1.hongkongpost.gov.hk/crl/eCertCA1-14CRL1.crl which is a full CRL issued by the Sub CA "Hongkong Post e-Cert CA 1 - 14".

11. URL of CRL Distribution Point for certificates issued by Sub CA "Hongkong Post e-Cert CA 1 - 15" is:

    http://crl1.hongkongpost.gov.hk/crl/eCertCA1-15CRL1.crl which is a full CRL issued by the Sub CA "Hongkong Post e-Cert CA 1 - 15".

12. URL of OCSP responder is: http://ocsp1.hongkongpost.gov.hk

Appendix C - Hongkong Post Certificate Revocation Lists (CRLs), Authority Revocation List (ARL) and Online Certificate Status Protocol (OCSP) Response Format

The Appendix C of this CPS provides the arrangement of updating and publishing as well as the format of the Certificate Revocation Lists (CRLs) that are issued by the Sub CAs "Hongkong Post e-Cert CA 1 - 10", "Hongkong Post e-Cert CA 1 - 14" and "Hongkong Post e-Cert CA 1 - 15", and the Authority Revocation List (ARL) that is issued by the root CA "Hongkong Post Root CA 1".

HKPost has delegated OCSP signing for the root CA "Hongkong Post Root CA 1" to an OCSP responder by issuing an OCSP signer's certificate containing the subject name "Hongkong Post Root CA 1 OCSP Responder". The OCSP signing for the Sub CA "Hongkong Post e-Cert CA 1 - 15" is delegated to an OCSP responder by issuing an OCSP signer's certificate containing the subject name "Hongkong Post e-Cert CA 1 - 15 OCSP Responder". Furthermore, a unique OID "**1.3.6.1.4.1.16030.1.6**" is assigned to the OCSP responders and specified in the field "Certificate Policies" of the OCSP signer's certificate. In the last section of this Appendix C, the format of OCSP response is also provided.

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

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

   i. e-Cert (Personal):
   http://crl1.hongkongpost.gov.hk/crl/eCertCA1-10CRL1_<xxxxx>.crl issued by the Sub CA "Hongkong Post e-Cert CA 1 - 10" where <xxxxx> is a string of five alphanumeric characters.
   ii. e-Cert (Organisational) and e-Cert (Encipherment):
   http://crl1.hongkongpost.gov.hk/crl/eCertCA1-10CRL2.crl issued by the Sub CA "Hongkong Post e-Cert CA 1 - 10".
   iii. e-Cert (Server):
   The information of suspended or revoked e-Cert (Server) certificates will only be published in the full CRL of the respective Sub CAs.

b) **Full CRLs** that contain Information of all suspended or revoked certificates that are issued by the Sub CA "Hongkong Post e-Cert CA 1 - 10", "Hongkong Post e-Cert CA 1 - 14" and "Hongkong Post e-Cert CA 1 - 15" respectively. Each of the full CRLs is available at the following locations (URLs):

   i. Certificates issued by Sub CA "Hongkong Post e-Cert CA 1 - 10" :
   http://crl1.hongkongpost.gov.hk/crl/eCertCA1-10CRL1.crl or
   ldap://ldap1.hongkongpost.gov.hk (port 389, cn=Hongkong Post e-Cert CA 1 - 10 CRL1, o=Hongkong Post, c=HK)

   ii. Certificates issued by Sub CA "Hongkong Post e-Cert CA 1 - 14" :
   http://crl1.hongkongpost.gov.hk/crl/eCertCA1-14CRL1.crl or
   ldap://ldap1.hongkongpost.gov.hk (port 389, cn=Hongkong Post e-Cert CA 1 - 14 CRL1, o=Hongkong Post, c=HK)

iii. Certificates issued by Sub CA "Hongkong Post e-Cert CA 1 - 15" : http://crl1.hongkongpost.gov.hk/crl/eCertCA1-15CRL1.crl or ldap://ldap1.hongkongpost.gov.hk (port 389, cn=Hongkong Post e-Cert CA 1 - 15 CRL1, o=Hongkong Post, c=HK)

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

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

(I) Format of Partitioned and Full CRL issued by the Sub CA "Hongkong Post e-Cert CA 1 - 10" under this CPS:

Standard Fields	Sub-fields	Field Contents of Partitioned CRL	Field Contents of Full CRL	Remarks
Version		v2		This field describes the version of encoded CRL as X.509 v2.
Signature algorithm ID		sha1RSA		This field contains the algorithm identifier for the algorithm used to sign the CRL.
Issuer name		cn=Hongkong Post e-Cert CA 1 - 10, o=Hongkong Post, c=HK		This field identifies the entity who has signed and issued the CRL.
This update		[UTC time]		"This Update" indicates the date the CRL was generated.
Next update		[UTC time]		"Next Update" contains the date by which the next CRL will be issued, but it will not be issued any later than the indicated date. Notwithstanding this, the CRL is updated and issued on a **daily** basis as stated in the CPS.
Revoked certificates	**User certificate**	[Certificate Serial Number]		Revoked certificates are listed by their serial numbers.
	Revocation date	[UTC time]		The date on which the revocation occurred is specified.
	CRL entry extensions			
	Reason code	[Revocation Reason Code]		(Note 1)
Standard extension (Note 2)				
Authority key identifier	**Issuer**	cn=Hongkong Post Root CA 1 o=Hongkong Post c=HK		This field provides a means of identifying the Public Key corresponding to the Private Key used to sign a CRL.
	Serial number	[Inherited from Issuer]		This field indicates the serial number of the issuer certificate.
CRL number		[Generated by CA system – each partitioned CRL has its own sequence]		The CRL Number is generated in sequence for each CRL issued by a CA.

Standard Fields	Sub-fields	Field Contents of Partitioned CRL	Field Contents of Full CRL	Remarks
Issuer distribution point		[DER Encoded CRL Distribution Point] **(This field will be set Critical.)**	Not used	This field is used for Partitioned CRLs only.

(II) Format of Full CRL issued by the Sub CA "Hongkong Post e-Cert CA 1 - 14" under this CPS :

Standard Fields	Sub-fields	Field Contents of Full CRL	Remarks
Version		v2	This field describes the version of encoded CRL as X.509 v2.
Signature algorithm ID		sha256RSA	This field contains the algorithm identifier for the algorithm used to sign the CRL.
Issuer name		cn=Hongkong Post e-Cert CA 1 - 14, o=Hongkong Post, c=HK	This field identifies the entity who has signed and issued the CRL.
This update		[UTC time]	"This Update" indicates the date the CRL was generated.
Next update		[UTC time]	"Next Update" contains the date by which the next CRL will be issued, but it will not be issued any later than the indicated date. Notwithstanding this, the CRL is updated and issued on a **daily** basis as stated in the CPS.
Revoked certificates	**User certificate**	[Certificate Serial Number]	Revoked certificates are listed by their serial numbers.
	Revocation date	[UTC time]	The date on which the revocation occurred is specified.
	CRL entry extensions		
	Reason code	[Revocation Reason Code]	(Note 1)
Standard extension (Note 2)			
Authority key identifier	**Issuer**	cn=Hongkong Post Root CA 1 o=Hongkong Post c=HK	This field provides a means of identifying the Public Key corresponding to the Private Key used to sign a CRL.
	Serial number	[Inherited from Issuer]	This field indicates the serial number of the issuer certificate.
CRL number		[Generated by CA system]	The CRL Number is generated in sequence for each CRL issued by a CA.

(III) Format of Full CRL issued by the Sub CA "Hongkong Post e-Cert CA 1 - 15" under this CPS :

Standard Fields	Sub-fields	Field Contents of Full CRL	Remarks
Version		v2	This field describes the version of encoded CRL as X.509 v2.
Signature algorithm ID		sha256RSA	This field contains the algorithm identifier for the algorithm used to sign the CRL.

Standard Fields	Sub-fields	Field Contents of Full CRL	Remarks
Issuer name		cn=Hongkong Post e-Cert CA 1 - 15, o=Hongkong Post, l=Hong Kong, s=Hong Kong, c=HK	This field identifies the entity who has signed and issued the CRL.
This update		[UTC time]	"This Update" indicates the date the CRL was generated.
Next update		[UTC time]	"Next Update" contains the date by which the next CRL will be issued, but it will not be issued any later than the indicated date. Notwithstanding this, the CRL is updated and issued on a **daily** basis as stated in the CPS.
Revoked certificates	**User certificate**	[Certificate Serial Number]	Revoked certificates are listed by their serial numbers.
	Revocation date	[UTC time]	The date on which the revocation occurred is specified.
	CRL entry extensions		
	Reason code	[Revocation Reason Code]	(Note 1)
Standard extension (Note 2)			
Authority key identifier	**Issuer**	cn=Hongkong Post Root CA 1 o=Hongkong Post c=HK	This field provides a means of identifying the Public Key corresponding to the Private Key used to sign a CRL.
	Serial number	[Inherited from Issuer]	This field indicates the serial number of the issuer certificate.
CRL number		[Generated by CA system]	The CRL Number is generated in sequence for each CRL issued by a CA.

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

http://crl1.hongkongpost.gov.hk/crl/RootCA1ARL.crl or ldap://ldap1.hongkongpost.gov.hk (port 389, cn=Hongkong Post Root CA 1, o=Hongkong Post, c=HK)

(IV) Format of ARL issued by the root CA "Hongkong Post Root CA 1" under this CPS :

Standard Fields	Sub-fields	Field Contents of ARL	Remarks
Version		v2	This field describes the version of encoded ARL as X.509 v2.
Signature algorithm ID		sha1RSA	This field contains the algorithm identifier for the algorithm used to sign the ARL.
Issuer name		cn=Hongkong Post Root CA 1 o=Hongkong Post, c=HK	This field identifies the entity who has signed and issued the ARL.
This update		[UTC time]	"This Update" indicates the date the ARL was generated.

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

(V) Format of OCSP response under this CPS :

HKPost OCSP responder only supports basic OCSP response type. A definitive OCSP response data is composed of:

Standard Fields	Sub-fields	Sub-fields	Field Contents	Remarks
Response data	Version		v1 (0x0)	
	Responder ID	by key	[SHA-1 hash of responder's public key]	
	Produced At		[GeneralizedTime]	Time at which this response was signed (GMT+0).
	Sequence of Single Response			
	Single Response	Certificate ID	[Requested certificate identifier]	Requested certificate identifier consists of: • Hash algorithm ID • Hash of Issuer's Subject Name • Hash of Issuer's public key • Certificate serial number
		Certificate status	[Status of certificate]	Good, Revoked (with date and time (GMT+0) and revocation reason code (Note 1)), Unknown.
		This update	[GeneralizedTime]	Date and Time the certificate status was last known to be correct (GMT+0).

Standard Fields	Sub-fields	Sub-fields	Field Contents	Remarks
		Next update	[GeneralizedTime]	Date and Time for new updates to be made available (GMT+0).
Signature algorithm ID			sha256RSA	Algorithm that was used to sign this response.
Signature			[Signature data]	Signature of this response
Certificate			[Responder signing certificate data]	Responder's signing certificate

Note

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

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

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

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

Appendix D - Summary of Hongkong Post e-Cert Features

1) e-Cert (Personal) Certificate

Features	**e-Cert (Personal) Certificates**	**e-Cert (Personal) with MR Status Certificates**	**e-Cert (Personal) Certificates issued to persons aged under 18**
Subscribers	Holders of valid HKID Card who are 18 or above		Holders of valid HKID Card who are under 18
Reliance Limit	HK$200,000		HK$0
Recognized Certificate	Yes		
Key pair size	2048-bit RSA		
Key pair generation	By HKPost on behalf of the Subscriber through the central key generation service.		
Identity verification	Authentication of the Applicant's identity		
Usage of certificate	Digital Signature and Encryption	Digital Signature	Digital Signature and Encryption
Subscriber's information included in the certificate	▪ English name as appeared on the HKID Card; ▪ HKID number encrypted as a hash value; ▪ Email address; and ▪ Subscriber Reference Number (SRN) generated by the HKPost CA system		
Subscription Fees	$50 per certificate (both new and renewal application) per year (see also Section 2.4 of this CPS)	See Section 2.4 of this CPS	$50 per certificate (both new and renewal application) per year (see also Section 2.4 of this CPS)
Certificate Validity	Three Years	One year or Two years or Three years	Three years
	(See Section 1.2.4, 3.2 and 3.3.1 of this CPS.)		

2) e-Cert (Organisational), e-Cert (Encipherment) and e-Cert (Server) Certificate

Features	e-Cert (Organisational) Certificates	e-Cert (Organisational) with MR Status Certificates	e-Cert (Encipherment) Certificates	e-Cert (Server) Certificates	e-Cert (Server) Certificates with Wildcard feature or Multi-domain feature
Subscribers	Organisations that hold a valid business registration certificate(Note 1) issued by the Government of the Hong Kong SAR, statutory bodies of Hong Kong whose existence is recognized by the laws of Hong Kong and bureaux, departments or agencies of Government of HKSAR				
Certificate Holders	Authorised Users who are members or employees of the Organisation as the Subscriber		Authorised Units of the Organisation as the Subscriber	Same as Subscriber	
Reliance Limit	HK$200,000				
Recognized Certificate	Yes				
Key pair size	2048-bit RSA				
Key pair generation	By HKPost on behalf of the Subscriber through the central key generation service.			Key generation by Subscriber	
Identity verification	Authentication of the identity of the organisation and its Authorised Representative			Authentication of the identity of the domain name, the organisation, and its Authorised Representative	
Usage of certificate	Digital Signature and Encryption	Digital Signature	Encryption only	Digital Signature (Note 2), Encryption	Digital Signature, Encryption
Subscriber's information included in the certificate	▪ Subscriber Organisation's name, including its Chinese name if provided ▪ Authorised User's name and email address ▪ Subscriber Reference Number (SRN) generated by the HKPost system ▪ Subscriber Organisation's company/business registration information(Note 3)		▪ Subscriber Organisation's name ▪ Authorised Unit's name and email address ▪ Subscriber Reference Number (SRN) generated by the HKPost system ▪ Subscriber Organisation's company/business registration information	▪ Subscriber Organisation's name ▪ Subscriber Organisation's server name ▪ Subscriber Reference Number (SRN) generated by the HKPost system ▪ Subscriber Organisation's company/business registration information	▪ Subscriber Organisation's name ▪ Subscriber Organisation's server name and additional server names listed in the Subject Alternative Name field ▪ Subscriber Reference Number (SRN) generated by the HKPost system ▪ Subscriber Organisation's company / business registration information

Features	e-Cert (Organisational) Certificates	e-Cert (Organisational) with MR Status Certificates	e-Cert (Encipherment) Certificates	e-Cert (Server) Certificates	e-Cert (Server) Certificates with Wildcard feature or Multi-domain feature
Subscription Fees and Administration Fees	(see Section 2.4 of this CPS)				
Certificate Validity	One year or two years	One year or two years or three years	One year or two years or three years or four years	One year or two years	One year or two years
	(see Sections 1.2.4 and 3.4.1 of this CPS)				

Note

1. For subscribers of e-Cert (Organisational) apart from the subscribers of e-Cert (Organisational) with MR Status, organisations that hold a valid certification letter issued by the Inland Revenue Department of the Government of Hong Kong SAR to Reporting Financial Institution as referred in Inland Revenue Ordinance (Cap. 112) are also acceptable (see Section 1.2.3.2).
2. This usage of digital signature is only applicable to e-Cert (Server) issued by Sub CA "Hongkong Post e-Cert CA 1 - 15" only.
3. For organisations that hold a valid certification letter issued by the Inland Revenue Department of the Government of Hong Kong SAR to Reporting Financial Institution as referred in Inland Revenue Ordinance (Cap. 112), only the IRD Reference Number of the certification letter will be included in the certificate.

Appendix E - List of Registration Authorities for the Hongkong Post e-Cert, if any

With effect from the date of this CPS, no Registration Authority for Hongkong Post e-Cert is appointed.

Appendix F - List of Subcontractor(s) of Certizen Limited for Hongkong Post e-Cert Services, if any

With effect from the date of this CPS, no Subcontractor of Certizen Limited for Hongkong Post e-Cert Services, for the purpose of this CPS, is appointed.

Appendix G - Lifespan of CA root certificates

Name of the root certificate	Lifespan	Remarks
Hongkong Post Root CA 1	15 May 2003 – 15 May 2023	
Hongkong Post e-Cert CA 1	15 May 2003 – 15 May 2013	This Sub CA ceased to issue e-Cert with effect from 26 February 2010.
Hongkong Post e-Cert CA 1 - 10	9 January 2010 – 15 May 2023	This Sub CA commences to issue e-Cert to applicants with effect from 26 February 2010.
Hongkong Post e-Cert CA 1 - 14	30 November 2014 – 15 May 2023	This Sub CA commences to issue e-Cert to applicants with effect from 1 January 2015.
Hongkong Post e-Cert CA 1 - 15	4 July 2015 – 15 May 2023	This Sub CA commences to issue e-Cert to applicants with effect from 1 September 2015.

Appendix H – List of Particular Applications and Corresponding Application-specific Codes for Hongkong Post e-Cert

Name of Particular Relying Party	Particular Application	Classes of Certificate	Application-specific code as defined in DNS field of Subject Alternative Name field in Certificate
Inland Revenue Department of the Government of the Hong Kong SAR	AEOI (Note 1) Portal	e-Cert (Organisational) except e-Cert (Organisational) with MR Status	"IRD_AEOI"

Note

1. AEOI stands for Automatic Exchange of Financial Account Information

Appendix I - Table of Comparison of Request for Comments ("RFC") 3647 and this CPS

Disclaimer: The comparison table provided below is intended for the convenience of cross-referencing between the RFC 3647 and this CPS and for the purpose of complying with the requirement as specified in Section IV. 1. (3) of the MRCP. The provisions of this CPS shall always prevail whenever contradiction in meaning arises between this CPS and the RFC 3647, and Subscriber or any relying party shall not hold HKPCA liable for loss and damage that they would sustain due to such contradiction or their reliance of the comparison table provided below.

For the avoidance of doubt, the sections that are marked with "Not Applicable" are due to the fact that those practices / services are not provided by HKPCA or they are irrelevant to HKPCA's current practices / services.

Sections of RFC3647	**Relevant sections of this CPS**	**Explanations**
1. Introduction	1	
1.1 Overview	1.1	
1.2 Document Name and Identification	1.1	
1.3 PKI Participants	1.2	
1.3.1 Certification Authorities	1.2.1	
1.3.2 Registration Authorities	2.1.2 and Appendix E	
1.3.3 Subscribers	1.2.2 and 1.2.3	
1.3.4 Relying Parties	1.2.2	
1.3.5 Other participants	2.1.3 and Appendix F	
1.4 Certificate Usage	1.2.3	
1.4.1 Appropriate Certificate Uses		
1.4.2 Prohibited Certificate Uses		
1.5 Policy Administration	Preamble and 8	
1.5.1 Organization Administering the Document	Preamble and 8	
1.5.2 Contact Person	1.3	
1.5.3 Person Determining CPS Suitability for the Policy	Preamble and 8	
1.5.4 CPS Approval Procedures	8	
1.6 Definition and Acronyms	Appendix A	
2. Publication and Repository Responsibilities	2.1.1 and 2.5	
2.1 Repositories	2.5.4	
2.2 Publication of Certification Information	2.5	
2.3 Time or Frequency of Publication	2.5	
2.4 Access Controls on Repositories	2.5.1 and 2.5.2	
3. Identification and Authentication	3	
3.1 Naming	3.1	
3.1.1 Type of Names	3.1.1	

Sections of RFC3647	Relevant sections of this CPS	Explanations
3.1.2 Need for Names to be Meaningful	3.1.2	
3.1.3 Anonymity or Pseudonymity of Subscribers	Not Applicable	This CPS does not accept anonymous or pseudonymous applicants.
3.1.4 Rules for Interpreting Various Name Forms	3.1.3	
3.1.5 Uniqueness of Names	3.1.4	
3.1.6 Recognition, Authentication, and Role of Trademarks	3.1.5 and 3.1.6	
3.2 Initial Identity Validation	3.1	
3.2.1 Method to Prove Possession of Private Key	3.1.7	
3.2.2 Authentication of Organization Identity	3.1.8	
3.2.3 Authentication of Individual Identity	3.1.9	
3.2.4 Non-Verified Subscriber Information	Not Applicable	This CPS does not disclose the contents of this section in accordance with RFC2527. Relevant information has been provided in Appendix B.
3.2.5 Validation of Authority	3.1.9	
3.2.6 Criteria for Interoperation	1.1	
3.3 Identification and Authentication for Re-Key Requests	3.3 and 3.4	Certificate Re-Key will take place during Certificate Renewal process.
3.3.1 Identification and Authentication for Routine Re-Key	3.3 and 3.4	
3.3.2 Identification and Authentication for Re-Key After Revocation	3.3 and 3.4	
3.4 Identification and Authentication for Revocation Request	4.6.2	
4. Certificate Life-Cycle Operational Requirements	4	
4.1 Certificate Application	4.1 - 4.4	
4.1.1 Who Can Submit a Certificate Application	4.1 - 4.4	
4.1.2 Enrollment Process and Responsibilities	2.1 and 4.1 - 4.4	
4.2 Certificate Application Processing	4.1 - 4.4	
4.2.1 Performing Identification and Authentication Functions	3.1.8 and 3.1.9	
4.2.2 Approval or Rejection of Certificate Applications	4.1 - 4.4	
4.2.3 Time to Process Certificate Applications	4.5	
4.3 Certificate Issuance	4.1 - 4.4	
4.3.1 CA Actions During Certificate Issuance	4.1 - 4.4	
4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate	4.1 - 4.4	
4.4 Certificate Acceptance	2.1.4 and 4.1 - 4.4	
4.4.1 Conduct Constituting Certificate Acceptance	4.1 - 4.4	
4.4.2 Publication of the Certificate by the CA	2.5 and 4.1 - 4.4	
4.4.3 Notification of Certificate Issuance by the CA to Other Entities	2.5 and 4.1 - 4.4	
4.5 Key Pair and Certificate Usage	2.1.4 and 2.1.6	

Sections of RFC3647	Relevant sections of this CPS	Explanations
4.5.1 Subscriber Private Key and Certificate Usage	2.1.4	
4.5.2 Relying Party Public Key and Certificate Usage	2.1.6	
4.6 Certificate Renewal	3.2 - 3.4	
4.6.1 Circumstances for Certificate Renewal	3.3 and 3.4	
4.6.2 Who May Request Renewal	3.3 and 3.4	
4.6.3 Processing Certificate Renewal Requests	3.3 and 3.4	
4.6.4 Notification of New Certificate Issuance to Subscriber	4.1 - 4.4	
4.6.5 Conduct Constituting Acceptance of a Renewal Certificate	4.1 - 4.4	
4.6.6 Publication of the Renewal Certificate by the CA	2.5 and 4.1 - 4.4	
4.6.7 Notification of Certificate Issuance by the CA to Other Entities	2.5 and 4.1 - 4.4	
4.7 Certificate Re-Key	3.2 - 3.4	Certificate Re-Key will take place during Certificate Renewal process.
4.7.1 Circumstances for Certificate Re-Key	3.3 and 3.4	
4.7.2 Who May Request Certification of a New Public Key	3.3 and 3.4	
4.7.3 Processing Certificate Re-Keying Requests	3.3 and 3.4	
4.7.4 Notification of New Certificate Issuance to Subscriber	4.1 - 4.4	
4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate	4.1 - 4.4	
4.7.6 Publication of the Re-Keyed Certificate by the CA	2.5 and 4.1 - 4.4	
4.7.7 Notification of Certificate Issuance by the CA to Other Entities	2.5 and 4.1 - 4.4	
4.8 Certificate Modification	Not Applicable	This CPS does not allow modification of an issued e-Cert.
4.8.1 Circumstances for Certificate Modification		
4.8.2 Who May Request Certificate Modification		
4.8.3 Processing Certificate Modification Requests		
4.8.4 Notification of New Certificate Issuance to Subscriber		
4.8.5 Conduct Constituting Acceptance of Modified Certificate		
4.8.6 Publication of the Modified Certificate by the CA		
4.8.7 Notification of Certificate Issuance by the CA to Other Entities		
4.9 Certificate Revocation and Suspension	4.6	
4.9.1 Circumstances for Revocation	2.1.4, 4.6.1 and 4.11.2	
4.9.2 Who Can Request Revocation	4.6.2	
4.9.3 Procedure for Revocation Request	4.6.2	
4.9.4 Revocation Request Grace Period	4.6.2	
4.9.5 Time Within Which CA Must Process the Revocation Request	4.6.3	
4.9.6 Revocation Checking Requirements for Relying Parties	2.1.6 and 4.6.4	
4.9.7 CRL Issuance Frequency	4.6.3 and 4.11.2	
4.9.8 Maximum Latency for CRLs	4.6.3	

Sections of RFC3647	Relevant sections of this CPS	Explanations
4.9.9 On-Line Revocation/Status Checking Availability	Not Applicable	Online status checking is currently not provided.
4.9.10 On-Line Revocation Checking Requirements	Not Applicable	Online status checking is currently not provided.
4.9.11 Other Forms of Revocation Advertisements Available	Not Applicable	Other forms of revocation advertisements are currently not provided.
4.9.12 Special Requirements re Key Compromise	Not Applicable	This service is currently not provided.
4.9.13 Circumstances for Suspension	2.1.4 and 4.6.2	
4.9.14 Who Can Request Suspension	4.6.2	
4.9.15 Procedure for Suspension Request	4.6.2	
4.9.16 Limits on Suspension Period	4.6.2	
4.10 Certificate Status Services	4.6.3 and 4.6.4	
4.10.1 Operational Characteristics	4.6.3	
4.10.2 Service Availability	4.6.3	
4.10.3 Operational Features	4.6.3	
4.11 End of Subscription	4.7	
4.12 Key Escrow and Recovery	6.2.3	
4.12.1 Key Escrow and Recovery Policy and Practices	6.2.3	
4.12.2 Session Key Encapsulation and Recovery Policy and Practices	6.2.3	
5. Facility, Management, and Operational Controls	2.1.4, 2.1.6, 4 and 5	
5.1 Physical Controls	5.1	
5.1.1 Site Location and Construction	5.1.1	
5.1.2 Physical Access	5.1.2	
5.1.3 Power and Air Conditioning	5.1.4	
5.1.4 Water Exposures	5.1.5	
5.1.5 Fire Prevention and Protection	5.1.6	
5.1.6 Media Storage	5.1.7	
5.1.7 Waste Disposal	5.1.10	
5.1.8 Off-site Backup	5.1.8	
5.2 Procedural Controls	5.2	
5.2.1 Trusted Roles	5.2.1	
5.2.2 Number of Personnel Needed for Each Task	5.2.1	
5.2.3 Identification and Authentication of Each Role	5.2.1	
5.2.4 Roles requiring Segregation of Duties	5.2.1	
5.3 Personnel Controls	5.3	
5.3.1 Qualifications, Experience, and Clearance Requirements	5.3.1	
5.3.2 Background Check Procedures	5.3.2	
5.3.3 Training Requirements	5.3.3	

Sections of RFC3647	Relevant sections of this CPS	Explanations
5.3.4 Retraining Frequency and Requirements	5.3.3	
5.3.5 Job Rotation Frequency and Sequence	Non-disclosure	This CPS does not disclose the contents of this section in accordance with the internal policy.
5.3.6 Sanctions for Unauthorised Actions	5.3.4	
5.3.7 Independent Contractor Requirements	Non-disclosure	This CPS does not disclose the contents of this section in accordance with the internal policy.
5.3.8 Documentation Supplied to Personnel	5.3.5	
5.4 Audit Logging Procedures	4.8	
5.4.1 Types of Events Recorded	4.8.1	
5.4.2 Frequency of Processing Log	4.8.2	
5.4.3 Retention Period for Audit Log	4.8.3	
5.4.4 Protection of Audit Log	4.8.4	
5.4.5 Audit Log Backup Procedures	4.8.5	
5.4.6 Audit Collection System (Internal vs. External)	4.8.6	
5.4.7 Notification to Event-Causing Subject	4.8.7	
5.4.8 Vulnerability Assessments	4.8.8	
5.5 Records Archival	4.9	
5.5.1 Types of Records Archived	4.9.1	
5.5.2 Retention Period for Archive	4.9.2	
5.5.3 Protection of Archive	4.9.3	
5.5.4 Archive Backup Procedures	4.9.4	
5.5.5 Requirements for Time-Stamping of Records	4.9.5	
5.5.6 Archive Collection System (Internal or External)	4.9.4	
5.5.7 Procedures to Obtain and Verify Archive Information	4.9.4	
5.6 Key Changeover	4.10	
5.7 Compromise and Disaster Recovery	4.11	
5.7.1 Incident and Compromise Handling Procedures	4.11	
5.7.2 Computing Resources, Software, and/or Data Are Corrupted	4.11.4	
5.7.3 Entity Private Key Compromise Procedures	4.11.2	
5.7.4 Business Continuity Capabilities After a Disaster	4.11.1	
5.8 CA or RA Termination	4.12 and 4.13	
6. Technical Security Controls	6	
6.1 Key Pair Generation and Installation	6.1	
6.1.1 Key Pair Generation	6.1.1 and 6.1.5	
6.1.2 Private Key Delivery to Subscriber	6.1.3	
6.1.3 Public Key Delivery to Certificate Issuer	6.1.2	

Sections of RFC3647	Relevant sections of this CPS	Explanations
6.1.4 CA Public Key Delivery to Relying Parties	4.1 - 4.4	
6.1.5 Key Sizes	6.1.4	
6.1.6 Public Key Parameters Generation and Quality Checking	6.1.5	
6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)	6.1.6	
6.2 Private Key Protection and Cryptographic Module Engineering Controls	6.2 and 6.7	
6.2.1 Cryptographic Module Standards and Controls	6.2.1 and 6.7	
6.2.2 Private Key (n out of m) Multi-Person Control	6.2.2	
6.2.3 Private Key Escrow	6.2.3	
6.2.4 Private Key Backup	6.2.4	
6.2.5 Private Key Archival	Non-disclosure	This CPS does not disclose the contents of this section in accordance with the internal policy.
6.2.6 Private Key Transfer between Cryptographic Modules	6.2.5	
6.2.7 Private Key Storage on Cryptographic Module	6.2.5	
6.2.8 Method of Activating Private Key	6.2.4	
6.2.9 Method of Deactivating Private Key	6.2.2	
6.2.10 Method of Destroying Private Key	Non-disclosure	This CPS does not disclose the contents of this section in accordance with the internal policy.
6.2.11 Cryptographic Module Rating	6.2.1 and 6.7	
6.3 Other Aspects of Key Pair Management	6.3	
6.3.1 Public Key Archival	6.3	
6.3.2 Certificate Operational Periods and Key Pair Usage Periods	6.3	
6.4 Activation Data	6.1 and 6.2	
6.4.1 Activation Data Generation and Installation		
6.4.2 Activation Data Protection		
6.4.3 Other Aspects of Activation Data		
6.5 Computer Security Controls	6.4	
6.5.1 Specific Computer Security Technical Requirements	6.4	
6.5.2 Computer Security Rating	6.4	
6.6 Life Cycle Technical Controls	6.5	
6.6.1 System Development Controls	6.5	
6.6.2 Security Management Controls	6.5	
6.6.3 Life Cycle Security Controls	6.5	
6.7 Network Security Controls	6.6	
6.8 Time-Stamping	Not Applicable	Not provided
7. Certificate, CRL, and OCSP Profiles	7	

Sections of RFC3647	Relevant sections of this CPS	Explanations
7.1 Certificate Profile	7.1	
7.1.1 Version Number(s)	Appendix B	
7.1.2 Certificate Extensions	Appendix B	
7.1.3 Algorithm Object Identifiers	Appendix B	
7.1.4 Name Forms	Appendix B	
7.1.5 Name Constraints	Appendix B	
7.1.6 Certificate Policy Object Identifier	Appendix B	
7.1.7 Usage of Policy Constraints Extension	Appendix B	
7.1.8 Policy Qualifiers Syntax and Semantics	Appendix B	
7.1.9 Processing Semantics for the Critical Certificate Policies Extension	Appendix B	
7.2 CRL Profile	7.2	
7.2.1 Version Number(s)	Appendix C	
7.2.2 CRL and CRL Entry Extensions	Appendix C	
7.3 OCSP Profile	7.3	For e-Cert (Server) issued by Sub CA "Hongkong Post e-Cert CA 1 - 15" only.
7.3.1 Version Number(s)	Appendix C	
7.3.2 OCSP Extensions	Appendix C	
8. Compliance Audit and Other Assessments	2.6	
8.1 Frequency and Circumstances of Assessment	2.6	
8.2 Identity/Qualifications of Assessor	2.6	
8.3 Assessor's Relationship to Assessed Entity	2.6	
8.4 Topics Covered by Assessment	2.6	
8.5 Actions Taken as a Result of Deficiency	Non-disclosure	This CPS does not disclose the contents of this section in accordance with the internal policy.
8.6 Communications of Results	Non-disclosure	This CPS does not disclose the contents of this section in accordance with the internal policy.
9. Other Business and Legal Matters	2	
9.1 Fees	2.4	
9.1.1 Certificate Issuance or Renewal Fees	2.4.1 - 2.4.4	
9.1.2 Certificate Access Fees	2.4.1 - 2.4.4	
9.1.3 Revocation or Status Information Access Fees	2.4.1 - 2.4.4	
9.1.4 Fees for Other Services	2.4.1 - 2.4.4	
9.1.5 Refund Policy	2.4.1 - 2.4.4	
9.2 Financial Responsibility	2.2.15	
9.2.1 Insurance Coverage	2.2.15	
9.2.2 Other Assets	2.2.15	
9.2.3 Insurance or Warranty Coverage for End-Entities	2.2.15	

Sections of RFC3647	Relevant sections of this CPS	Explanations
9.3 Confidentiality of Business Information	2.7	
9.3.1 Scope of Confidential Information	2.7	
9.3.2 Information Not Within the Scope of Confidential Information	2.7	
9.3.3 Responsibility to Protect Confidential Information	2.7	
9.4 Privacy of Personal Information	2.7	
9.4.1 Privacy Plan	2.7	
9.4.2 Information Treated as Private	2.7	
9.4.3 Information Not Deemed Private	2.7	
9.4.4 Responsibility to Protect Private Information	2.7	
9.4.5 Notice and Consent to Use Private Information	Not Applicable	This CPS does not disclose the contents of this section in accordance with RFC2527.
9.4.6 Notice and Consent to Use Private Information	2.7	
9.4.7 Other Information Disclosure Circumstances	2.7	
9.5 Intellectual Property rights	1.2.2.1	
9.6 Representations and Warranties	2	
9.6.1 CA Representations and Warranties	2.2.3	
9.6.2 RA Representations and Warranties	2.1.1	
9.6.3 Subscriber Representations and Warranties	2.1.4	
9.6.4 Relying Party Representations and Warranties	2.1.6	
9.6.5 Representations and Warranties of Other Participants	Not Applicable	This CPS does not disclose the contents of this section in accordance with RFC2527.
9.7 Disclaimers of Warranties	2.2.10	
9.8 Limitations of Liability	2.2.3	
9.9 Indemnities	2.2.3	
9.10 Term and Termination	Not Applicable	Currently not defined
9.10.1 Term		
9.10.2 Termination		
9.10.3 Effect of Termination and Survival		
9.11 Individual Notices and Communications with Participants	2.3.2	
9.12 Amendments	8	
9.12.1 Procedure for Amendment	8	
9.12.2 Notification Mechanism and Period	8	
9.12.3 Circumstances Under Which OID Must be Changed	8	
9.13 Dispute Resolution Provisions	2.3.3	
9.14 Governing Law	2.3.1	

Sections of RFC3647	Relevant sections of this CPS	Explanations
9.15 Compliance with Applicable Law	2.3.1	
9.16 Miscellaneous Provisions	2.3	
9.16.1 Entire Agreement	2.3.2	
9.16.2 Assignment	2.2.5	
9.16.3 Severability	2.3.2	
9.16.4 Enforcement (Attorney's Fees and Waiver of Rights)	2.3.3	
9.17 Other Provisions	Not Applicable	This CPS does not disclose the contents of this section in accordance with RFC2527.