THE CERTIFICATION PRACTICE STATEMENT

OF

THE POSTMASTER GENERAL

As

**A Recognized Certification Authority
under the Electronic Transactions Ordinance**

for

Hongkong Post e-Cert (Server)

Date :   31 August 2020
OID : 1.3.6.1.4.1.16030.1.7.7

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 of the People's Republic of China ("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 January 2020 to 30 June 2022.

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 G**. 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, and publication in a publicly available Repository of recognized and accepted digital certificates for secure on-line identification. The SSL/TLS certificates issued under this CPS (i.e. e-Cert (Server)) 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, except the functions of domain name validation. A list of Registration Authorities, if any, can be found in **Appendix F**.

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.

This CPS conforms to RFC3647 Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework.

This CPS is designed to meet the latest version of the requirements of the following schemes:
- the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates ("Baseline Requirements") published by the CA / Browser Forum;
- WebTrust Principles and Criteria for Certification Authorities;
- WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security;

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 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.

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 (Server) certificates issued under this CPS as Recognized Certificates.** This means for both Subscribers and Relying Parties, that HKPost has a legal obligation under the Ordinance to use a Trustworthy System for the issuance, revocation 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.

This CPS meets the format requirements of RFC 3647. While certain section titles are included in this CPS according to the structure of RFC 3647, the topic may not necessarily apply to services of HKPost. These sections state 'No stipulation'. Additional information is presented in subsections of the standard structure where necessary. Meeting the format requirements of RFC 3647 enhances and facilitates the mapping and interoperability with other third party CAs and provides Relying Parties with advance notice of HKPost's practices and procedures.

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

1.2   Document Name and Identification

This document is the HKPost CA Certification Practice Statement ("CPS"). The following revisions have been made since the creation of this document.

Revision Number	Revision Description	Effective Date
1	First version to replace the existing Certification Practice Statement (OID 1.3.6.1.4.1.16030.1.1.37) for issuing e-Cert (Server) in alignment with RFC 3647.	31 May 2018

Revision Number	Revision Description	Effective Date
2	To update Section 4.2.1 to comply with BR domain validation practices	30 July 2018
3	To update the period of the outsource HKPost CA operation contract.	31 October 2018
4	To fix the description of certificate revocation and suspension process; To update PREAMBLE such that "RAs carry out certain of the functions of HKPost except the functions of domain name validation"; and To update Section 4.9.1 for inclusion of all revocation reasons as required by BR.	1 February 2019
5	To issue e-Cert (Server) under Root CA 3 and change certificate format related to change of HKPCA domain name	1 July 2019
6	To update the period of the outsource HKPost CA operation contract.	1 January 2020
7	To only issue certificates with 1-year validity period in accordance with major browsers' root certificate policy, which requires the lifetimes of TLS server certificates to be no more than 398 days.	31 August 2020

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**") **"1.3.6.1.4.1.16030.1.7.7"** (see description of the field "Certificate Policies" in **Appendix B**). In addition to this OID, all certificates that comply with the Baseline Requirements will include one of the following additional identifiers, which are assigned by the CA / Browser Forum:-

> **"2.23.140.1.2.2"** of the Organisation Validation SSL certificates

1.3   PKI Participants

1.3.1   Certification Authorities

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

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, 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.

HKPost, as a Recognized CA, is responsible under the Ordinance for the use of a Trustworthy System for the issuance, revocation 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:

Hongkong Post e-Cert
香港郵政電子核證

a) issue and publish certificates in a timely manner (see Section 2.3);

b) notify Applicants of the approval or rejection of their applications (see Sections 4.1 to 4.4);

c) revoke certificates and publish Certificate Revocation Lists and provide OCSP responses in a timely manner (see Section 4.9); and

d) notify Subscribers of the revocation of their certificates (see Section 4.9.5).

1.3.2 Registration Authorities

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 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.**

Refer to **Appendix F** - List of Registration Authorities for the Hongkong Post e-Cert, if any.

1.3.3 Subscribers

Under this CPS, a Subscriber is the "Subscriber" or "Subscriber Organisation" referred to in **Appendix A**. 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 any way for the issue of those e-Certs (see also Section 1.3.2). Subscribers who rely on an e-Cert of another Subscriber in a transaction will be Relying Parties in respect of such a certificate.

Classes of Subscribers

HKPost issues one class of certificates under this CPS, e-Cert (Server), 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.

Ordinary e-Cert (Server) 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 SAR 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. Such certificates are validated according to Organisation Validation rules in compliance to CA / Browser Forum Baseline Requirements.

1.3.4 Relying Parties

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 Registration Authorities.

1.3.5 Other participants

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.

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.

Refer to **Appendix G** - List of Subcontractor(s) of Certizen Limited for Hongkong Post e-Cert Services.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

HKPost issues e-Cert (Server) certificates under this CPS only to Applicants whose application for a certificate has been approved by HKPost and who have signed or confirmed their acceptance of a Subscriber Agreement in the appropriate form.

E-Cert (Server) certificates 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 certificate are to be used only for server authentication and for establishment of secure communication channels with the server. The digital signatures generated by the certificate are under no circumstances to be used for negotiation or conclusion of a contract or any legally binding agreement or any monetary transactions.

1.4.2 Prohibited Certificate Uses

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.

1.5 Policy Administration

1.5.1 Organisation Administering the Document

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

1.5.2 Contact Person

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@eCert.gov.hk

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.

1.5.3 Person Determining CPS Suitability for the Policy

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.

1.5.4 CPS Approval Procedures

All changes to this CPS must be approved and published by HKPost. HKPost has the right to vary this CPS without notice (see Section 9.12).

1.6 Definition and Acronyms

Refer to **Appendix A** – Glossary and Acronyms.

2. Publication and Repository Responsibilities

2.1 Repositories

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 (Server) 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 public 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 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 communications.

2.2 Publication of Certification Information

The HKPost Repository can be accessed at URLs as follows:

http://www.eCert.gov.hk
ldap://ldap1.eCert.gov.hk
or alternatively
http://www.hongkongpost.gov.hk
ldap://ldap1.hongkongpost.gov.hk

2.3 Time or Frequency of Publication

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. 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.

HKPost reviews this CPS annually and update it if necessary. New or modified versions of this CPS is typically published within seven (7) days after its approval.

2.4 Access Controls on Repositories

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

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).

3. Identification and Authentication

3.1 Naming

3.1.1 Type of Names

3.1.1.1 Subject Name
The Subscriber Organisation for an e-Cert (Server) certificate can be 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 Government Department or 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. 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).

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).

3.1.1.2 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 (Server) certificate, that person will not be identified in the certificate.

3.1.1.3 Organisation Names in Chinese Language
E-Cert (Server) is issued in English language with the organisation name in either English or Chinese language. For organisations who subscribe to e-Cert (Server) and have provided their company's Chinese name in the application form, they may determine whether to display Chinese company name on the e-Cert (Server). If the organisation fails to provide such distinction, the company's English name shall be displayed on the e-Cert (Server). For organisations who subscribe to e-Cert (Server) and are companies with company names in the Chinese language only or who have provided their company's Chinese name only, the company's Chinese name shall be displayed on the e-Cert (Server).

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 Anonymity or Pseudonymity of Subscribers

HKPost does not issue anonymous or pseudonymous certificates for server authentication.

3.1.4 Rules for Interpreting Various Name Forms

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

3.1.5 Uniqueness of Names

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. Domain name uniqueness is controlled by the Internet Corporation for Assigned Names and Numbers (ICANN).

3.1.6 Recognition, Authentication, and Role 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, domain name, trade name, company name, or any other intellectual property rights of any third party.

The decisions of HKPost in matters concerning any disputes concerning the ownership of trademarks, service marks, domain name, trade name, company name, or any other intellectual property rights are discretionary and final.

3.2 Initial Identity Validation

All Applicants for e-Cert (Server) shall submit a completed and signed application form to HKPost. The e-Cert (Server) certificate applications require the Authorised Representative of the organisation to complete and sign the application form and the organisation will become a Subscriber. 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 3.2.2. Following approval of the application, HKPost prepares an e-Cert (Server) and notifies the Applicant of how the certificate may be issued as described in Section 4.3.

3.2.1 Method to Prove Possession of Private Key

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.eCert.gov.hk.

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 Applicant's Private Keys.

3.2.2 Authentication of Organisation Identity

Applications for e-Cert (Server) 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

Hongkong Post e-Cert
香港郵政電子核證

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.

3.2.2.1 e-Cert (Server)
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 Government Department or 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;

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.

3.2.3 Authentication of Individual Identity
The Authorised Representative of organisational Applicant 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 3.2.2.

3.2.4 Non-Verified Subscriber Information
HKPost verifies the subject elements and the alternative subject name as defined in Section 7.1.4.2 of the CA / Browser Forum Baseline Requirements. Any other non-verified information included in an e-Cert (Server) is designated as such in the certificate, and HKPost shall not be responsible for non-verified Subscriber information submitted to HKPost.

3.2.5 Validation of Authority
Validation of authority involves a determination of whether the Authorised Representative has specific rights, entitlements, or permissions, including the permission to act on behalf of the Subscriber Organisation to obtain an e-Cert (Server).

For all applications of e-Cert (Server), the authority of the Authorised Representative is verified by using one or more of the procedures listed in Section 3.2.2.4 of the CA / Browser Forum

Baseline Requirements ("BR") and a Reliable Method of Communication in accordance with Section 3.2.5 of the BR.

3.2.6 Criteria for Interoperation

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

3.3 Identification and Authentication for Re-Key Requests

HKPost supports re-key of an existing certificate prior to the expiry of the certificate for two purposes, i.e.

i)   Replacement of a certificate, which is when some (or none) of the subject details have been changed after the application and the Subscriber may (or may not) wish to change the key associated with the new certificate;

ii) Renewal of a certificate, which is when the Subscriber wishes to extend the lifetime of an existing certificate and may also change the key associated with the certificate.

In both cases, a re-verification of identification and authentication as stipulated in Section 4.2.1 is required.

3.3.1 Identification and Authentication for Routine Re-Key

HKPost does not support routine re-key of certificate for replacement on request. Certificate re-key will ordinarily take place as part of a certificate renewal process, or on HKPost's discretionary as part of a certificate replacement process.

3.3.2 Identification and Authentication for Re-Key After Revocation

HKPost shall not permit re-key of expired or revoked certificates.

A Subscriber, or the Authorised Representative of a Subscriber Organisation must undergo the initial registration process as described in Section 3.2.

3.4 Identification and Authentication for Revocation Request

After receiving the revocation request from subscriber or through the RA to which the request for revocation was first submitted, HKPost shall validate the request and verify the justifications for revocation. 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 (1) an action on a confirmation web page by the Subscriber, after having its identity authenticated in the designated web page on the HKPost website where the request was submitted, (2) an email digitally signed by the Subscriber's Private Key, (3) an original letter signed by the Subscriber or (4) a Request for Certificate Revocation Form signed by the Subscriber.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

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.

4.1.1 Who Can Submit a Certificate Application

An Authorised Representative of Applicant that hold a valid business registration certificate issued by the Government of the Hong Kong SAR, statutory bodies of Hong Kong SAR whose existence is recognized by the laws of Hong Kong, or bureaux, departments or agencies of Government of HKSAR may submit a certificate application to HKPost.

4.1.2 Enrolment Process and Responsibilities

Applicants for e-Cert must complete the enrolment process, which includes:
  a) Complete and submit an application form at a designated HKPost premises or premises of other organisations designated by HKPost,
  b) Provide required supporting documents as stated in the application form during the enrolment process,
  c) Pay any applicable subscription fees,
  d) Generate the Private Key and public key,
  e) Generate the Certificate Signing Request (CSR) containing the public key, and transmits the CSR to HKPost through a designated web page at http://www.eCert.gov.hk.

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 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

The documentation required for proving the identity of the Subscriber Organisation and Authorised Representative(s) is stipulated in Sections 3.2.2 and 3.2.3 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 names, neither "eCert.gov.hk" nor "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).

With respect to the validation of domain authorisation 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); or

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 Authorisation 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).

4.2.2 Approval or Rejection of Certificate Applications

Following the identity verification process, HKPost has the obligation to notify Applicants of the approval or rejection of their applications. Applicants whose applications have been rejected may subsequently reapply. HKPost reserves right of refusal in its absolute discretion without incurring any liability or responsibility for any loss or expenses arising as a result of such refusal.

4.2.3 Time to Process 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 (Server)	Ten working days

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 4.2.3.

4.3   Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

Applicant's information is captured and reviewed by at least two HKPost staff who are capable of directly causing certificate issuance and have had logged in with two-factors authentication in HKPost's system. Following successful completion of all required validations of Applicant's certificate application, HKPost approves the application for e-Cert (Server).

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.

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.

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

Following the successful identity verification process, HKPost shall notify the Applicant approval of an application via email to the email address designated by the Subscriber during the application process.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance
The Applicant verifies and confirms the accuracy of the information contained in the e-Cert at the designated web page at http://www.eCert.gov.hk. If the Applicant rejects the e-Cert, HKPost shall revoke that e-Cert. A Subscriber is deemed to have accepted the e-Cert when the Subscriber uses the e-Cert.

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.

4.4.2 Publication of the Certificate by the CA
All issued and accepted e-Certs will be published in the Repository under the Ordinance.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities
RAs may receive notification of a certificate's issuance if the RA was involved in the issuance process.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage
Subscribers are responsible for:
a) 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.
b) 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).
c) Not using a certificate in a transaction on becoming aware of any ground upon which HKPost could revoke it under the terms of the CPS, or after the Subscriber has made a revocation request or been notified by HKPost of HKPost's intention to revoke the certificate under the terms of this CPS.
d) Upon becoming so aware of any ground upon which HKPost could revoke the certificate, or upon the Subscriber making a revocation request or upon being notified by HKPost of its intention to revoke the certificate, immediately notifying Relying Parties in any transaction that remains to be completed at the time, that the certificate used in that transaction is liable to be revoked (either by HKPost or at the 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.
e) For the purpose of identity authentication, using the Private Key of an e-Cert only during its validity period.

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.

Hongkong Post e-Cert
香港郵政電子核證

4.5.2 Relying Party Public Key and Certificate Usage

Relying Parties relying upon e-Cert (Server) 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 F**) 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) Performing all appropriate certificate path validation procedures.

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

4.6 Certificate Renewal

4.6.1 Circumstances for Certificate Renewal

HKPost shall notify Subscribers to renew their e-Cert (Server) 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 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 6.3.2:

Validity period of a new certificate	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

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.

4.6.2 Who May Request Renewal

There is no automatic certificate renewal of an e-Cert (Server) certificates. The process of "Authentication of Organisation Identity" as described under Section 3.2.2 of this CPS 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.eCert.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.

4.6.3 Processing Certificate Renewal Requests

Renewal application requirements and procedures are generally the same as those used during the certificate original issuance. The process of "Authentication of Organisation Identity" as described under Section 3.2.2 will be conducted. HKPost requires that the Subscriber does re-key for the new certificate.

4.6.4 Notification of New Certificate Issuance to Subscriber
Notification to the Subscriber about the issuance of a renewed certificate is given using the same means as a new e-Cert, described in Section 4.3.2 of this CPS.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate
Subscriber's conduct constituting acceptance of a renewal e-Cert is the same as listed in Section 4.4.1 of this CPS.

4.6.6 Publication of the Renewal Certificate by the CA

HKPost publishes a renewed e-Cert in the same way as a new e-Cert, described in Section 4.4.2 of this CPS.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities
RAs may receive notification of a certificate's renewal if the RA was involved in the issuance process.

4.7   Certificate Re-Key

4.7.1 Circumstances for Certificate Re-Key
Re-keying a certificate consists of creating a new certificate with a new Public Key and serial number while keeping the subject information the same. Certificate re-key will ordinarily take place as part of a certificate renewal process, or on HKPost's discretionary as part of a certificate replacement process.

4.7.2 Who May Request Certification of a New Public Key
HKPost will only accept re-key requests from the same Subscriber of the e-Cert, or HKPost at its discretion. However, HKPost will not renew, or request re-keying, an e-Cert (Server) certificate automatically.

4.7.3 Processing Certificate Re-Keying Requests
The procedure of processing a certificate re-key requests may be the same as issuing a new certificate.

4.7.4 Notification of New Certificate Issuance to Subscriber
HKPost will notify Subscriber of a certificate re-key by the means delineated in Section 4.3.2 of this CPS.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate
Subscriber's conduct constituting acceptance of a re-keyed certificate is the same as listed in Section 4.4.1 of this CPS.

4.7.6 Publication of the Re-Keyed Certificate by the CA
HKPost publishes a re-keyed e-Cert in the same way as a new e-Cert, described in Section 4.4.2 of this CPS.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities
RAs may receive notification of a certificate's re-key if the RA was involved in the issuance process.

4.8   Certificate Modification
This CPS does not allow modification of an issued e-Cert.

4.8.1 Circumstances for Certificate Modification
No stipulation.

4.8.2 Who May Request Certificate Modification
No stipulation.

4.8.3 Processing Certificate Modification Requests
No stipulation.

4.8.4 Notification of New Certificate Issuance to Subscriber
No stipulation.

4.8.5 Conduct Constituting Acceptance of Modified Certificate
No stipulation.

4.8.6 Publication of the Modified Certificate by the CA
No stipulation.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities
No stipulation.

4.9 Certificate Revocation and Suspension
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 5.7.3).

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. Suspension of a certificate is not applicable.

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.

4.9.1 Circumstances for Revocation
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 or any change in the Information in the certificate provided by the Subscriber.

HKPost will revoke an e-Cert (Server) in accordance with the procedures in the CPS within 24 hours whenever it:

1) receives a request for revocation of an e-Cert (Server) through a designated web page on the HKPost web site at http://www.eCert.gov.hk from a Subscriber;
2) is notified from a Subscriber that the original application of e-Cert (Server) was not authorised and does not retroactively grant authorisation;
3) knows or reasonably suspects that a Subscriber's Private Key has been compromised; or
4) knows or reasonably suspects that any details upon an e-Cert (Server) are not true or

have become untrue or that the e-Cert (Server) is otherwise unreliable, including but not limited to that the validation of domain authorisation or control for any FQDN in the e-Cert (Server) should not be relied upon.

HKPost may revoke an e-Cert (Server) within 24 hours and will revoke an e-Cert (Server) within 5 days in accordance with the procedures in the CPS whenever it:

5) receives a request for revocation of an e-Cert (Server) by fax, letter mail, email, in-person from a Subscriber;
6) determines that an e-Cert (Server) no longer complies with the requirements of Sections 6.1.5 and 6.1.6 of the CA/Browser Forum baseline requirements in relation to key sizes and public key parameter generation and quality checking;
7) obtains evidence that an e-Cert (Server) was misused;
8) determines that the Subscriber had failed to meet any of the obligations set out in this CPS or the Subscriber Agreement;
9) knows or reasonably suspects any circumstance indicating that use of a FQDN in the e-Cert (Server) is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name registrant and the Applicant has terminated, or the Domain Name registrant has failed to renew the Domain Name);
10) knows or reasonably suspects that a Wildcard e-Cert (Server) has been used to authenticate a fraudulently misleading subordinate FQDN;
11) knows or reasonably suspects a material change in the information contained in an e-Cert (Server);
12) determines that an e-Cert (Server) was not properly issued in accordance with the CA/Browser Forum baseline requirements or this CPS;
13) determines, or knows or reasonably suspects that any of the information appearing in an e-Cert (Server) is inaccurate;
14) is required to do so when HKPost's right to issue certificate under CA/Browser Forum baseline requirements expires or is revoked or terminated, unless HKPost has made arrangements to continue maintaining the CRL and/or OCSP repository;
15) is required to do so by this CPS, any regulation, or law applicable to the e-Cert (Server) ;
16) determines that the Subscriber has failed to pay the subscription fee;
17) determines that a demonstrated or proven method that exposes the Subscriber's Private Key to compromise, methods have been developed that can easily calculate it based on the Public Key (such as a Debian weak key, see http://wiki.debian.org/SSLkeys), or if there is clear evidence that the specific method used to generate the Private Key was flawed;
18) 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) is no longer owned by the Subscriber Organisation; or
19) knows or has reasonable cause to believe that the Subscriber whose details appear on an e-Cert (Server) 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.

Currently all Sub CA Certificates under this CPS are operated by HKPost only. Revocation of a Sub CA Certificate shall be performed within seven (7) days if one or more of the following occurs:

1) HKPost obtains evidence that the Sub CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Sections 6.1.5 and 6.1.6 of the CA/Browser Forum baseline requirements in relation to key sizes and public key parameter generation and quality checking;

2) HKPost obtains evidence that the Sub CA Certificate was misused;

3) HKPost confirms that the Sub CA Certificate was not issued in accordance with the CA/Browser Forum baseline requirements or this CPS;

4) HKPost determines that any of the information appearing in the CA Certificate is inaccurate or misleading;

5) HKPost ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the CA Certificate;

6) HKPost's right to issue Certificates under the Baseline Requirements expires or is revoked or terminated, unless HKPost has made arrangements to continue maintaining the CRL/OCSP Repository;

7) Revocation is required by HKPost's CPS; or

8) The technical content or format of the Sub CA Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties.

4.9.2 Who Can Request Revocation

A Subscriber, or the Authorised Representative of a Subscriber Organisation, may submit a certificate revocation request to HKPost by fax, letter mail, email, in-person or through a designated web page on the HKPost web site at http://www.eCert.gov.hk. Additionally, Subscribers, Relying Parties, Application Software Suppliers, and other third parties may submit Certificate Problem Reports informing HKPost of reasonable cause to revoke an e-Cert (Server). Certificate Problem Reports must identify the entity requesting revocation and specify the reason with supporting evidence for revocation. HKPost may revoke a certificate without receiving a request and without prior notice.

4.9.3 Procedure for Revocation Request

After receiving the revocation request, HKPost shall validate the request and verify the justifications for revocation. 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 (1) an action on a confirmation web page by the Subscriber, after having its identity authenticated in the designated web page on the HKPost website where the request was submitted, (2) an email digitally signed by the Subscriber's Private Key, (3) an original letter signed by the Subscriber or (4) a Request for Certificate Revocation Form signed by the Subscriber. HKPost 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 revocation ("Notice of Revocation") in accordance with the procedures in the CPS. If the certificate supports OCSP, the OCSP response for that certificate will remain revoked after the certificate expires. The Request for Certificate Revocation Form can be obtained from the web site at http://www.eCert.gov.hk.

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.

4.9.4 Revocation Request Grace Period

The revocation request grace period ("Grace Period") means the period during which the Subscriber must make a revocation request. 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 or any change in the Information in the certificate provided by the Subscriber.

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 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.

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 revoke a certificate (either in response to a request or otherwise) and the appearance of the revocation status on the Certificate Revocation List, or in the period between that decision to 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.

4.9.5 Time within Which CA Must Process the Revocation Request

For submission of certificate revocation request to HKPost through a designated web page on the HKPost web site, the revocation would be reflected in CRL within 24 hours. For requests

by other methods, HKPost shall exercise reasonable endeavours to ensure that within 24 hours starting from the next working date 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 revoke the certificate, the revocation is posted to the Certificate Revocation List. However, a Certificate Revocation List is not immediately published in the directory for access by the public following each certificate revocation. Only when the next Certificate Revocation List is updated and published will it reflect the revoked status of the certificate. Certificate Revocation Lists are published 3 times daily and are archived for at least 7 years. On the contrary, if the certificate supports OCSP, the OCSP response for that certificate will be updated and published immediately to reflect the revocation status of that certificate.

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 24 hours following the revocation.

4.9.6 Revocation Checking Requirements for Relying Parties
Relying Parties before relying upon this certificate are responsible for checking the status of this certificate on the Certificate Revocation List, or the relevant OCSP response whenever applicable, prior to reliance.

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.

HKPost's policy concerning the situation where a Relying Party is temporarily unable to obtain Information on revoked certificate is stipulated in Section 9.6.4 (Relying Parties Representations and Warranties) and Section 9.7 (Disclaimers of Warranties) of this CPS.

4.9.7 CRL Issuance Frequency
When an e-Cert is revoked, HKPost shall publish the relevant information (including the Certificate Revocation List (such as Authority Revocation List of HKPost) on a timely basis.

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

4.9.8 Maximum Latency for CRLs
HKPost does not employ a maximum latency for CRLs. Generally, however, CRLs for e-Cert are posted automatically to the Repository within a commercially reasonable time after generation.

4.9.9 On-Line Revocation/Status Checking Availability
The OCSP response for certificates will be updated and published immediately to reflect the revocation status of the certificate in accordance with the format specified in **Appendix D**.

4.9.10 On-Line Revocation Checking Requirements
Relying Party's must confirm the validity of a certificate in accordance with Section 4.9.6 prior to relying on the certificate.

4.9.11 Other Forms of Revocation Advertisements Available
No stipulation.

4.9.12 Special Requirements Related to Key Compromise
No stipulation.

4.9.13 Circumstances for Suspension
Not applicable.

4.9.14 Who Can Request Suspension
Not applicable.

4.9.15 Procedure for Suspension Request
Not applicable.

4.9.16 Limits on Suspension Period
Not applicable.

4.10 Certificate Status Services

4.10.1 Operational Characteristics
The information of all certificates that have been revoked, including the reason code identifying the reason for the certificate revocation, will be included in the Certificate Revocation List (see Section 7.2). Furthermore, their certificate status with the reason code will be included in the OCSP response for each individual certificate (see Section 7.3).

4.10.2 Service Availability
Certificate status services are available 24x7.

4.10.3 Operational Features
No stipulation.

4.11 End of 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 Retention Period for Archive specified in Section 5.5.2.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices
No private key escrow process is planned for HKPost Private Keys and Subscribers' Private Keys in the e-Cert system used by HKPost.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices
No stipulation.

5. Facility, Management, and Operational Controls

5.1 Physical Controls

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

5.1.4 Water Exposures
The CA facility is protected to the extent reasonably possible from natural disasters. HKPost CA has also established handling procedures to protect the systems from damages or other adverse consequences arising from flooding or water leakage.

5.1.5 Fire 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.

5.1.6 Media Storage
Media storage and disposition processes have been developed and are in place. For paper documents including Subscriber Agreements and photocopies of identity confirmation documents, they are maintained by HKPost, the Contractor or its RAs in a secure fashion. Only authorised personnel are permitted access to the paper records.

5.1.7 Waste Disposal
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.

5.1.8 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 5.7.4).

5.2   Procedural Controls

5.2.1 Trusted Roles
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.

5.2.2 Number of Personnel Needed for Each Task
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.

5.2.3 Identification and Authentication of Each Role
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.

5.2.4 Roles requiring Segregation of Duties
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.

5.3   Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements
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 Check Procedures
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 Retraining Frequency and Requirements

HKPost, the Contractor or its RAs 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.

5.3.5 Job Rotation Frequency and Sequence

No stipulation

5.3.6 Sanctions for Unauthorised Actions

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.

5.3.7 Independent Contractor Requirements

The Contractor personnel who are assigned to perform trusted roles are subject to the duties and requirements specified for such roles in this Section 5.3 and are subject to sanctions stated above in Section 5.3.6.

5.3.8 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.

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.

5.4 Audit Logging Procedures

5.4.1 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 requests
  - Actual issuance and revocation of certificates
  - Certificate renewals
  - Updates to repositories
  - CRL generation and posting
  - OCSP response signing and generation
  - CA Key rollover
  - Backups
  - Emergency key recoveries

5.4.2 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.

5.4.3 Retention Period for Audit Log
Archived audit log files are retained for at least 7 years.

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

5.4.5 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.

5.4.6 Audit Collection System (Internal vs. External)
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.

5.4.7 Notification to Event-Causing Subject
HKPost has an automated process in place to report critical audited events to the appropriate person or system.

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

5.5 Records Archival

5.5.1 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.

5.5.2 Retention Period for Archive
Key and certificate information as well as archival records as specified in Section 5.5.1 are securely maintained for at least 7 years. Audit trail files are maintained in the CA system as deemed appropriate by HKPost.

5.5.3 Protection of Archive
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.

5.5.4 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.

5.5.5 Requirements for Time-Stamping of Records
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.

5.5.6 Archive Collection System (Internal or External).
Archive information is collected internally by HKPost.

5.5.7 Procedures to Obtain and Verify Archive Information
Details concerning the procedures to obtain and verify archive information are found in Section 5.5.4.

5.6 Key Changeover
The lifespan of the HKPost CA and e-Cert root keys and certificates created by HKPost (See **Appendix H**) for the purpose of certifying certificates issued under this CPS is no more than 25 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.eCert.gov.hk for public access. The original root keys will be kept for a minimum period as specified in Section 5.5.2 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.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures
HKPost maintains incident handling procedures to guide personnel in response to security incidents, natural disasters, and similar events that may give rise to system compromise. To

Hongkong Post e-Cert
香港郵政電子核證

maintain the integrity of certificate services, HKPost implements, documents, and periodically tests appropriate contingency and disaster recovery plans and procedures.

5.7.2 Computing Resources, Software, and/or Data Are Corrupted
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 (Server) 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.

5.7.3 Entity Private Key Compromise Procedures
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 (Server) 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.

In the event of key compromise or disaster where a HKPost Private Key for the issuance of e-Cert (Server) 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.

5.7.4 Business Continuity Capabilities after a Disaster
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.

5.8 CA or RA 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.

In the event that the RA is terminated under RA agreement or under CA termination as stated above 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.

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.

Signing key generation, storage, and signing operations performed by HKPost are conducted within a hardware cryptographic module that is rated to at least FIPS 140-1 Level 3.

6.1.2 Private Key Delivery to Subscriber

The Applicant's Private Key will be generated by the Applicant.

6.1.3 Public Key Delivery to Certificate Issuer

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.

6.1.4 CA Public Key Delivery to Relying Parties

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

6.1.5 Key Sizes

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

6.1.6 Public Key Parameters Generation and Quality Checking

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

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

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 and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

The cryptographic devices used by HKPost are rated to at least FIPS 140-1 Level 3.

6.2.2 Private Key (n out of m) 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 Private Key Backup

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.

6.2.5 Private Key Archival

All Private Keys will not be archived.

6.2.6 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 authorisation.

6.2.7 Private Key Storage on Cryptographic Module

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

6.2.8 Method of Activating Private Key

Details concerning method of activating private key are found in Section 6.2.2.

6.2.9 Method of Deactivating Private Key

Details concerning method of deactivating private key are found in Section 6.2.2.

6.2.10 Method of Destroying Private Key

HKPost CA root keys will be used for no more than 25 years (see also Section 5.6). 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 5.5.

6.2.11 Cryptographic Module Rating

Details concerning cryptographic module rating can be found in Section 6.2.1 of this CPS.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Key and certificate information as well as archival records as specified in Section 5.5.1 are securely maintained for at least 7 years.

HKPost CA root keys will be used for no more than 25 years (see also Section 5.6). All HKPost key generation, key destruction, key storage, certificate revocation list signing operations, and

Hongkong Post e-Cert
香港郵政電子核證

OCSP signing operations are performed in a hardware cryptographic module. Archival of HKPost Public Keys is performed as specified in Section 5.5.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

HKPost CA root keys will be used for no more than 25 years (see also Section 5.6). 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 5.5.

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 (Server), including e-Cert (Server) with Wildcard feature or Multi-domain feature	1 year

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 Section 4.6). The validity period of an e-Cert is specified in the certificate itself. Format of certificates issued under this CPS is in **Appendix B**.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

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.

6.4.2 Activation Data Protection

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.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

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 8. 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.

6.5.2 Computer Security Rating
No stipulation

6.6 Life Cycle Technical Controls

6.6.1 System Development 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).

6.6.2 Security Management Controls
HKPost implements controls over the procedures for changes of security-related configurations and security software of its CA systems. These procedures include checking the integrity of the application and security software.

6.6.3 Life Cycle Security Controls
No stipulation

6.7 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.

6.8 Time-Stamping
The system time on HKPost's computers is updated using the Network Time Protocol (NTP) to synchronize system clocks with a reliable time service at least once every eight hours (Windows default). HKPost does not provide any time-stamping service to public.

7. Certificate, CRL, and OCSP 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. A summary of the features of the e-Cert (Server) certificates is in **Appendix E**.

7.1.1 Version Number(s)

All certificates referred to in this CPS are issued in the X.509 version 3 format (See **Appendix B**).

7.1.2 Certificate Extensions

The format of certificates referred to in this CPS is in **Appendix B**.

7.1.3 Algorithm Object Identifiers

The format of certificates referred to in this CPS is in **Appendix B**.

7.1.4 Name Forms

The format of certificates referred to in this CPS is in **Appendix B**.

7.1.5 Name Constraints

The format of certificates referred to in this CPS is in **Appendix B**.

7.1.6 Certificate Policy Object Identifier

The format of certificates referred to in this CPS is in **Appendix B**.

7.1.7 Usage of Policy Constraints Extension

The format of certificates referred to in this CPS is in **Appendix B**.

7.1.8 Policy Qualifiers Syntax and Semantics

The format of certificates referred to in this CPS is in **Appendix B**.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

The format of certificates referred to in this CPS is in **Appendix B**.

7.2 CRL Profile

HKPost updates and publishes the following Certificate Revocation Lists (CRLs) containing information of e-Certs 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)).

Details concerning the CRL profile can be found in **Appendix C**.

7.2.1 Version Number(s)

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

7.2.2 CRL and CRL Entry Extensions

Details concerning the CRL and CRL entry extensions can be found in **Appendix C**.

7.3 OCSP Profile

HKPost has delegated OCSP signing for the root CAs and the following Sub CAs to an OCSP responder by issuing the respective OCSP signer's certificate containing the subject name as follows:

Root CA

Certificate subject name (CN)	OCSP signer's certificate subject name (CN)
"Hongkong Post Root CA 1"	"Hongkong Post Root CA 1 OCSP Responder"
"Hongkong Post Root CA 3"	"Hongkong Post Root CA 3 OCSP Responder"

Sub CA

Certificate subject name (CN)	OCSP signer's certificate subject name (CN)
"Hongkong Post e-Cert CA 1 - 15"	"Hongkong Post e-Cert CA 1 - 15 OCSP Responder"
"Hongkong Post e-Cert SSL CA 3 - 17"	"Hongkong Post e-Cert SSL CA 3 - 17 OCSP Responder"

Details concerning the OCSP profile can be found in **Appendix D**.

7.3.1 Version Number(s)

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

7.3.2 OCSP Extensions

Details concerning the OCSP extensions can be found in **Appendix D**.

8. Compliance Audit and Other Assessments

The practices in this CPS are designed to meet or exceed the requirements of industry standards such as the WebTrust for Certification Authorities. HKPost, as a Recognized CA, is required to prepare and submit an assessment report under Section 43(1) of the Ordinance.

8.1 Frequency and Circumstances of Assessment

Compliance audits and assessments are performed at least once in every 12 months.

8.2 Identity/Qualifications of Assessor

Qualification of the independent external auditor conducting compliance assessments are in accordance with the requirements set out in the Ordinance and the Code of Practice for Recognized Certification Authorities. WebTrust auditor must meet the requirements of Section 8.2 of the CA / Browser Forum Baseline Requirements.

8.3 Assessor's Relationship to Assessed Entity

Compliance assessments are performed by an independent external auditor that is independent from HKPost in accordance with the requirements set out in the Ordinance and the Code of Practice for Recognized Certification Authorities.

8.4 Topics Covered by Assessment

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

8.5 Actions Taken as a Result of Deficiency

If an audit reports a material noncompliance with applicable law, this CPS, or any other contractual obligations related to HKPost's services, then (1) the auditor will document the discrepancy, (2) the auditor will promptly notify HKPost, and (3) depending on the nature and extent of the discrepancy, HKPost will create a suitable corrective action plan to cure the noncompliance and decide whether to take any remedial action with regard to e-Certs already issued.

8.6 Communications of Results

WebTrust for Certification Authorities audit report is made available to the public at http://www.eCert.gov.hk/product/cps/ecert. Compliance assessment report under Section 43(1) of the Ordinance is submitted to the Government Chief Information Officer.

8.7 Self-Audits

On at least a quarterly basis, HKPost performs self-audits against a randomly selected sample of at least 3 percent of the e-Certs issued since the last self-audit. Self-audits on e-Certs are performed in accordance with guidelines adopted by the CA / Browser Forum.

Hongkong Post e-Cert
香港郵政電子核證

9. Other Business and Legal Matters

9.1 Fees

The subscription fee and administration fee shall be paid before the commencement of each subscription period by e-Cert Subscribers unless waived by HKPost. HKPost may revoke an e-Cert if its subscription terminates during the validity period specified in the certificate (see also Section 4.9.1(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.eCert.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.

9.1.1 Certificate Issuance or Renewal Fees

Subscription Fees per certificate for e-Cert (Server) Certificates	Certificate with a 1-year validity period
New application or renewal of e-Cert (Server) for single server name	HK$2,500
New application or renewal of e-Cert (Server) with Wildcard feature	HK$8,700 + HK$500 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. Promotional discount on subscription fees for e-Cert (Server) with Wildcard feature certificates is offered by the Contractor. For details on the promotional discount, please refer to HKPost web site at http://www.eCert.gov.hk or make enquiry to Hongkong Post Certification Authority through the means provided in Section 1.5.2
New application or renewal of e-Cert (Server) with Multi-domain feature	HK$3,000 + HK$2,500 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.

9.1.2 Certificate Access Fees

HKPost may charge a reasonable fee for direct access to its certificate databases.

9.1.3 Revocation or Status Information Access Fees

HKPost does not charge a certificate revocation fee or a fee for checking the validity status of an issued certificate using a CRL or via OCSP.

Hongkong Post e-Cert
香港郵政電子核證

9.1.4 Fees for Other Services
No stipulation.

9.1.5 Refund Policy
Notwithstanding the limitation of HKPost's liability set out in Section 9.8, 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.

9.2   Financial Responsibility

9.2.1 Insurance Coverage
HKPost maintains commercial general liability insurance coverage of at least two million US dollars. Moreover, a separate insurance policy is also in place to cover the potential or actual liabilities and claims against Reliance Limit on the certificates pursuant to the provisions of ETO.

9.2.2 Other Assets
No stipulation

9.2.3 Insurance or Warranty Coverage for End-Entities
An insurance policy is in place to cover the potential or actual liabilities and claims against Reliance Limit on the certificates.

9.3   Confidentiality of Business Information

9.3.1 Scope of Confidential Information
Information about Subscribers that is submitted as part of an application for an e-Cert (Server) 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.

9.3.2 Information Not Within the Scope of Confidential Information
Any information not listed as confidential is considered public information. Published Certificate and revocation data is considered public information.

9.3.3 Responsibility to Protect Confidential Information
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, 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.

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.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan
HKPost has implemented a privacy policy, which complies with this CPS. The HKPost privacy policy is published at HKPost web site at http://www.eCert.gov.hk.

9.4.2 Information Treated as Private
Any information about subscribers that is not publicly available through the content of the issued certificate, repository and CRL is treated as private.

9.4.3 Information Not Deemed Private
Published certificate and revocation data is considered public information. Certificate status information and any certificate content is deemed not private.

9.4.4 Responsibility to Protect Private Information
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, 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.

9.4.5 Notice and Consent to Use Private Information
Information about Subscribers that is submitted as part of an application for an e-Cert (Server) 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.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process
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.

9.4.7 Other Information Disclosure Circumstances
No stipulation.

9.5 Intellectual Property rights
HKPost owns all intellectual property rights associated with its databases, web sites, e-Cert certificates, trademarks and any other publication originating from HKPost including this CPS.

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

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

HKPost publishes Recognized Certificates that are accepted by and issued to its Subscribers in a Repository (See Section 2).

By issuing a certificate that refers to this CPS, HKPost represents to Relying Parties who act in accordance with Section 9.6.4 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 9.6.4 and other relevant sections of this CPS that HKPost has issued the certificate to the Subscriber identified in it.

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.

9.6.2 RA Representations and Warranties

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 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.**

9.6.3 Subscriber Representations and Warranties

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

   a) No person other than the Subscriber of an e-Cert (Server) 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 1.4.
   d) All information and representations made by the Subscriber included in the certificate are true.

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

f) All information supplied in the certificate application process does not infringe or violate in any way the trademarks, service marks, trade name, company name, or any other intellectual property rights of any third party.

Subscribers are responsible for:

a) Completing the application procedures properly and signing, or confirming acceptance of, a Subscriber Agreement by the Authorised Representative in the appropriate form and performing the obligations placed upon them by that Agreement, and ensuring accuracy of representations in certificate application.

b) Accurately following the procedures specified in this CPS as to the expiry of certificates.

c) Notifying HKPost immediately from time to time of any change in the appointment and information of the Authorised Representative of e-Cert (Server) certificates.

d) Notifying HKPost immediately of any fact which may give rise to HKPost, upon the grounds set out in Section 4 of this CPS, having the right to revoke the certificate for which that Subscriber is responsible.

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

f) Upon becoming so aware of any ground upon which HKPost could revoke the certificate, or upon the Subscriber making a revocation request or upon being notified by HKPost of its intention to revoke the certificate, immediately notifying Relying Parties in any transaction that remains to be completed at the time, that the certificate used in that transaction is liable to be revoked (either by HKPost or at the 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.

g) 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.

h) For the purpose of identity authentication, using the Private Key of an e-Cert only during its validity period.

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.

9.6.4 Relying Party Representations and Warranties
Relying Parties relying upon e-Cert (Server) 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 F**) 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) Performing all appropriate certificate path validation procedures.

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

9.6.5 Representations and Warranties of Other Participants

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.

9.7 Disclaimers of Warranties

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.

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.

9.8 Limitations of Liability

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.

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**.

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 (Server) certificate.

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, 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.

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.

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.

9.9 Indemnities

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

None of the Hong Kong Post Office, the Contractor 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.

Time Limit For Making Claims
Any Relying Party who wishes to make any legal claim upon the Postmaster General arising out of or in any way connected with the issuance, 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."

9.10 Term and Termination

9.10.1 Term
The CPS changes will be effective upon publication by HKpost in the HKPost CA website at http://www.eCert.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.

9.10.2 Termination
This CPS, including all amendments and addenda, remain in force until replaced by a newer version.

9.10.3 Effect of Termination and Survival

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.

9.11   Individual Notices and Communications with Participants

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.

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@eCert.gov.hk

9.12   Amendments

9.12.1 Procedure for Amendment

Upon approval of an updated CPS by HKPost, the CPS changes will be effective upon publication by HKPost in the HKPost CA web site at http://www.eCert.gov.hk or in the HKPost Repository and are binding on all current and subsequent Applicants and Subscribers to whom certificates are issued.

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. 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.

9.12.2 Notification Mechanism and Period

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.eCert.gov.hk.

9.12.3 Circumstances Under Which OID Must be Changed

HKPost has the sole authority to determine whether an amendment to the CPS requires an OID change.

9.13   Dispute Resolution Provisions

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@eCert.gov.hk

9.14 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.

9.15 Compliance with Applicable 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.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

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

9.16.2 Assignment

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

9.16.3 Severability

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.

9.16.4 Enforcement (Attorney's Fees and Waiver of Rights)

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@eCert.gov.hk

9.16.5 Force Majeure

HKPOST INCURS NO LIABILITY IF IT IS PREVENTED, FORBIDDEN OR DELAYED FROM PERFORMING, OR OMITS TO PERFORM, ANY ACT OR REQUIREMENT BY REASON OF: ANY PROVISION OF ANY APPLICABLE LAW, REGULATION OR ORDER; CIVIL, GOVERNMENTAL OR MILITARY AUTHORITY; THE FAILURE OF ANY ELECTRICAL, COMMUNICATION OR OTHER SYSTEM OPERATED BY ANY OTHER PARTY OVER WHICH IT HAS NO CONTROL; FIRE, FLOOD, OR OTHER EMERGENCY CONDITION; STRIKE; ACTS OF TERRORISM OR WAR; ACT OF GOD; OR OTHER SIMILAR CAUSES BEYOND ITS REASONABLE CONTROL AND WITHOUT ITS FAULT OR NEGLIGENCE.

9.17 Other Provisions

9.17.1 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 Section 9.8. 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.

Appendix A – Glossary and Acronyms

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;

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

"Application Software Supplier" means a supplier of Internet browser software or other Relying Party application software that displays or uses Certificates and incorporates Hongkong Post Root Certificates.

"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.

"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 http://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 Problem Report" means a complaint of suspected key compromise, certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificate.

"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 January 2020 to 30 June 2022.

"Contractor" means Certizen Limited, together with its Subcontractor(s), if any as listed in **Appendix G**, 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" means a label assigned to a node in the Domain Name System.

"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).

"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.

"Fully-Qualified Domain Name" or "FQDN" means a Domain Name that includes the labels of all superior nodes in the Internet Domain Name System.

"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.

"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.

"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.

"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).

"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.

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

 "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 Agency" means a Governmental Agency that registers business information in connection with an entity's business formation or authorisation to conduct business under a license, charter or other certification.

"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.

"Reliable Method of Communication" means a method of communication, such as a postal/courier delivery address, telephone number, or email address, that was verified using a source other than the Authorised Representative.

"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.

"S/MIME" is the acronym of Secure/Multipurpose Internet Mail Extension(s).

"SSL" is the acronym of Secure Sockets Layer.

"Sub CA" means the subordinate Certification Authority certificate which is issued by the root CAs of HKPost 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 (Server) certificate has been issued in accordance with the eligibility criteria set out in this CPS.

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

"TLS" is the acronym of Transport Layer Security.

"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.

"WebTrust for Certification Authorities" means the current version of CPA Canada's WebTrust Program for Certification Authorities, published at http://www.webtrust.org/.

"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.

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", "Hongkong Post e-Cert CA 1 - 15" and "Hongkong Post e-Cert SSL CA 3 - 17" 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) Format of e-Cert (Server) Certificate under root CA "Hongkong Post Root CA 1"

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

(HKPCA has stopped to issue e-Cert (Server) under Sub CA "Hongkong Post e-Cert CA 1 - 10" since 1 January 2016.)

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]		

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**
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		
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):-

(HKPCA has stopped to issue e-Cert (Server) under Sub CA "Hongkong Post e-Cert CA 1 - 14" since 1 September 2016.)

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]		

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**
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		
	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):-

(HKPCA has stopped to issue e-Cert (Server) under Sub CA "Hongkong Post e-Cert CA 1 - 15" since 1 July 2019.)

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]		

HongkongPost e-Cert
香港郵政電子核證

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**
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]		
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] Policy Identifier =2.23.140.1.2.2 (Note 13) 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. *.eCert.gov.hk, *.subdomain.eCert.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 3.1.1.3 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 1.2 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. *.eCert.gov.hk and eCert.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.

13. The CA/Browser Forum OID is added in this field for identification of the certificate which is issued in compliance with CA / Browser Forum Baseline Requirements – organisation identity asserted.

2) Format of e-Cert (Server) Certificate under root CA "Hongkong Post Root CA 3"

For e-Cert (Server) issued by Sub CA "Hongkong Post e-Cert SSL CA 3 - 17" 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 SSL CA 3 - 17 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 10)		
Authority key identifier		[Subject Key Identifier of the issuer's certificate]		
Subject Key Identifier		[hash value of the Subject's public key]		
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] Policy Identifier =2.23.140.1.2.2 (Note 11) 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 9)		
1.3.6.1.4.1.11129.2.4.2		Signed Certificate Timestamp		

Note

1. The server name (including the domain name of the server) owned by the Subscriber Organisation. In addition to English server name, Chinese server name with characters encoded in ISO/IEC 10646 is also supported. 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. *.eCert.gov.hk, *.subdomain.eCert.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. e-Certs are issued in English language with the organisation names in either English or Chinese language. For organisations who subscribe to e-Cert and have provided their company's Chinese name in the application form, they may determine whether to display Chinese company name on the e-Cert. If the organisation fails to provide such distinction, the company's English name shall be displayed on the e-Cert. 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, the company's Chinese name shall be displayed on the e-Cert (see Section 3.1.1.3 of this CPS). Moreover, the organisation branch/department name will be displayed at the same language of the company name. All standard extensions are set as "non-critical" unless otherwise specified.

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

6. The OID of this CPS is included in this field. Please refer to Section 1.2 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. *.eCert.gov.hk and eCert.gov.hk). In addition to English server name, Chinese server name with characters encoded in ISO/IEC 10646 is also supported.

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). In addition to English server name, Chinese server name characters encoded in ISO/IEC 10646 is also supported.

9. URL of CRL Distribution Point for certificates issued by Sub CA "Hongkong Post e-Cert SSL CA 3 - 17" is:

   http://crl1.eCert.gov.hk/crl/eCertSCA3-17CRL1.crl which is a full CRL issued by the Sub CA "Hongkong Post e-Cert SSL CA 3 - 17".

10. URL of OCSP responder is: http://ocsp1.eCert.gov.hk

11. The CA/Browser Forum OID is added in this field for identification of the certificate which is issued in compliance with CA / Browser Forum Baseline Requirements – organisation identity asserted.

Appendix C - Hongkong Post Certificate Revocation Lists (CRLs) and Authority Revocation List (ARL)

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", "Hongkong Post e-Cert CA 1 - 15", "Hongkong Post e-Cert SSL CA 3 - 17" and the Authority Revocation List (ARLs) that are issued by the root CA "Hongkong Post Root CA 1" and "Hongkong Post Root CA 3".

With respect to Certificate Revocation Lists (CRLs), HKPost updates and publishes CRLs containing information of e-Certs 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) **Full CRLs** that contain Information of all revoked certificates that are issued by the Sub CAs "Hongkong Post e-Cert CA 1 - 10", "Hongkong Post e-Cert CA 1 - 14", "Hongkong Post e-Cert CA 1 - 15" and "Hongkong Post e-Cert SSL CA 3 - 17" 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)

   iv. Certificates issued by Sub CA "Hongkong Post e-Cert SSL CA 3 - 17" :
   http://crl1.eCert.gov.hk/crl/eCertSCA3-17CRL1.crl or
   ldap://ldap1.eCert.gov.hk (port 389, cn=Hongkong Post e-Cert SSL CA 3 - 17 CRL1, o=Hongkong Post, c=HK)

The URL for accessing the relevant CRL that contains the information of the 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.eCert.gov.hk/ on ad hoc basis without prior notice.

HKPost updates and publishes the Authority Revocation Lists (ARLs) containing information of revoked Sub CA certificates under this CPS annually before the next update date of the respective ARL or when necessary. The latest ARLs are available at the following locations:

i. Certificates issued by root CA "Hongkong Post Root CA 1" :
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)

ii. Certificates issued by root CA "Hongkong Post Root CA 3" :
http://crl1.eCert.gov.hk/crl/RootCA3ARL.crl or
ldap://ldap1.eCert.gov.hk (port 389, cn=Hongkong Post Root CA 3, o=Hongkong Post, c=HK)

(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.
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.
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.

Standard Fields	Sub-fields	Field Contents of Full CRL	Remarks
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.

(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.
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.

Standard Fields	Sub-fields	Field Contents of ARL	Remarks
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 Full CRL issued by the Sub CA "Hongkong Post e-Cert SSL CA 3 - 17" 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 SSL CA 3 - 17, 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 3 o=Hongkong Post l=Hong Kong, s=Hong Kong, 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.

(VI)   Format of ARL issued by the root CA "Hongkong Post Root CA 3" 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.

Standard Fields	Sub-fields	Field Contents of ARL	Remarks
Signature algorithm ID		sha256RSA	This field contains the algorithm identifier for the algorithm used to sign the ARL.
Issuer name		cn=Hongkong Post Root CA 3 o=Hongkong Post, l=Hong Kong, s=Hong Kong 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.
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 3 o=Hongkong Post l=Hong Kong, s=Hong Kong, 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.)**	

Appendix D - Hongkong Post Online Certificate Status Protocol (OCSP) Response Format

The Appendix D of this CPS provides the format of OCSP response:

HKPost has delegated OCSP signing for the root CAs and the following Sub CAs to an OCSP responder by issuing the respective OCSP signer's certificate containing the subject name as follows:

Root CA

Certificate subject name (CN)	OCSP signer's certificate subject name (CN)
"Hongkong Post Root CA 1"	"Hongkong Post Root CA 1 OCSP Responder"
"Hongkong Post Root CA 3"	"Hongkong Post Root CA 3 OCSP Responder"

Sub CA

Certificate subject name (CN)	OCSP signer's certificate subject name (CN)
"Hongkong Post e-Cert CA 1 - 15"	"Hongkong Post e-Cert CA 1 - 15 OCSP Responder"
"Hongkong Post e-Cert SSL CA 3 - 17"	"Hongkong Post e-Cert SSL CA 3 - 17 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 D, the format of OCSP response is also provided.

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).
		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

Standard Fields	Sub-fields	Sub-fields	Field Contents	Remarks
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.

Hongkong Post e-Cert
香港郵政電子核證

Appendix E - Summary of Hongkong Post e-Cert Features

1) e-Cert (Server) Certificate

Features	e-Cert (Server) Certificates
Subscribers	Organisations that hold a valid business registration certificate issued by the Government of the Hong Kong SAR, statutory bodies of Hong Kong SAR whose existence is recognized by the laws of Hong Kong and bureaux, departments or agencies of Government of HKSAR
Certificate Holders	Same as Subscriber
Reliance Limit	HK$200,000
Recognized Certificate	Yes
Key pair size	2048-bit RSA
Key pair generation	Key generation by Subscriber
Identity verification	Authentication of the identity of the domain name, the organisation, and its Authorised Representative
Usage of certificate	Digital Signature, Encryption
Subscriber's information included in the certificate	▪ 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
Subscription Fees and Administration Fees	(see Section 9.1 of this CPS)
Certificate Validity	One year (see Sections 4.6.1 and 6.3.2 of this CPS)

Appendix F - 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 G - 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 H - 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 ceased to issue e-Cert (Server) with effect from 1 January 2016.
Hongkong Post e-Cert CA 1 - 14	30 November 2014 - 15 May 2023	This Sub CA ceased to issue e-Cert (Server) with effect from 1 September 2016.
Hongkong Post e-Cert CA 1 - 15	4 July 2015 - 15 May 2023	This Sub CA ceased to issue e-Cert (Server) with effect from 1 July 2019.
Hongkong Post Root CA 3	12 August 2017 - 15 May 2023	This cross-certificate is issued to root CA "Hongkong Post Root CA 3" with effect from 12 August 2017.

Name of the root certificate	Lifespan	Remarks
Hongkong Post Root CA 3	3 June 2017 - 3 June 2042	This root CA commences to issue Sub CAs with effect from 3 June 2017.
Hongkong Post e-Cert SSL CA 3 - 17	3 June 2017 - 3 June 2032	This Sub CA commences to issue e-Cert to applicants with effect from 1 July 2019.

**THIS IS THE LAST PAGE OF
CERTIFICATION PRACTICE STATEMENT**