

THE CERTIFICATION PRACTICE STATEMENT

OF

THE POSTMASTER GENERAL

As

A Recognized Certification Authority under the Electronic Transactions Ordinance

for

Hongkong Post e-Cert (Organisational Role)

Date : 1 November 2026
OID : 1.3.6.1.4.1.16030.1.3.22

Table of Contents

PREAMBLE **4**
1. INTRODUCTION **6**
1.1 Overview 6
1.2 Community and Applicability 6
1.2.1 Certification Authority 6
1.2.2 Registration Authority 7
1.2.3 End Entities 7
1.2.4 Classes of Subscribers 8
1.2.5 Certificate Lifespan 8
1.2.6 Application at Premises Designated by HKPost 8
1.3 Contact Details 9
1.4 Complaints Handling Procedures 9
2. GENERAL PROVISIONS **10**
2.1 Obligations 10
2.1.1 CA Obligations 10
2.1.2 Registration Authority Obligations 10
2.1.3 Contractor Obligations 10
2.1.4 Registration Office Obligations 11
2.1.5 Subscriber Obligations 11
2.1.6 Relying Party Obligations 12
2.2 Further Provisions 12
2.2.1 Reasonable Skill and Care 12
2.2.2 No Supply of Goods 13
2.2.3 Limitation of Liability 13
2.2.4 HKPost's Liability for Received but Defective Certificates 16
2.2.5 Assignment by Subscriber 16
2.2.6 Authority to Make Representations 16
2.2.7 Variation 16
2.2.8 Retention of Title 16
2.2.9 Conflict of Provisions 17
2.2.10 Fiduciary Relationships 17
2.2.11 Cross Certification 17
2.2.12 Financial Responsibility 17
2.3 Interpretation and Enforcement (Governing Law) 17
2.3.1 Governing Law 17
2.3.2 Severability, Survival, Merger, and Notice 17
2.3.3 Dispute Resolution Procedures 17
2.3.4 Interpretation 17
2.4 Subscription Fees 17
2.5 Publication and Repository 17
2.5.1 Certificate Repository Controls 18
2.5.2 Certificate Repository Access Requirements 18
2.5.3 Certificate Repository Update Cycle 18
2.5.4 Permitted Use of Information Contained in the Repository 18
2.6 Compliance Assessment 18
2.7 Confidentiality 18
3. IDENTIFICATION AND AUTHENTICATION **19**
3.1 Initial Application 19
3.1.1 Types of Names 19
3.1.2 Need for Names to be Meaningful 19
3.1.3 Rules for Interpreting Various Names 19
3.1.4 Name Uniqueness 19
3.1.5 Name Claim Dispute Resolution Procedure 20
3.1.6 Infringement and Violation of Trademarks 20
3.1.7 Method to Prove Possession of the Private Key 20
3.1.8 Authentication of Identity of Organisational Applicant 20
3.2 Certificate Renewal 21
3.2.1 e-Cert (Organisational Role) certificates 21
3.2.2 Validity Period of Renewed e-Cert (Organisational Role) 21

4. OPERATIONAL REQUIREMENTS 22
4.1 Certificate Application 22
4.2 Certificate Issuance 22
4.3 Publication of e-Cert (Organisational Role) 22
4.4 Certificate Suspension and Revocation 22
4.4.1 Circumstances for Suspension and Revocation 22
4.4.2 Revocation Request Procedure 23
4.4.3 Service Pledge & Certificate Revocation List Update 24
4.4.4 Effect of Revocation 25
4.5 Computer Security Audit Procedures 25
4.5.1 Types of Events Recorded 25
4.5.2 Frequency of Processing Log 26
4.5.3 Retention Period for Audit Logs 26
4.5.4 Protection of Audit Logs 26
4.5.5 Audit Log Backup Procedures 26
4.5.6 Audit Information Collection System 26
4.5.7 Notification of Event-Causing Subject to HKPost 26
4.5.8 Vulnerability Assessments 26
4.6 Records Archival 26
4.6.1 Types of Records Archived 26
4.6.2 Archive Retention Period 26
4.6.3 Archive Protection 26
4.6.4 Archive Backup Procedures 27
4.6.5 Timestamping 27
4.7 Key Changeover 27
4.8 Disaster Recovery and Key Compromise Plans 27
4.8.1 Disaster Recovery Plan 27
4.8.2 Key Compromise Plan 27
4.8.3 Key Replacement 27
4.9 CA Termination 28
4.10 Registration Authority Termination 28
5. PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY CONTROLS 29
5.1 Physical Security 29
5.1.1 Site Location and Construction 29
5.1.2 Access Controls 29
5.1.3 Power and Air Conditioning 29
5.1.4 Natural Disasters 29
5.1.5 Fire Prevention and Protection 29
5.1.6 Media Storage 29
5.1.7 Off-site Backup 29
5.1.8 Protection of Paper Documents 29
5.2 Procedural Controls 29
5.2.1 Trusted Role 29
5.2.2 Transfer of Document and Data between HKPost, Contractors and RAs 29
5.2.3 Annual Assessment 30
5.3 Personnel Controls 30
5.3.1 Background and Qualifications 30
5.3.2 Background Investigation 30
5.3.3 Training Requirements 30
5.3.4 Documentation Supplied To Personnel 30
6. TECHNICAL SECURITY CONTROLS 31
6.1 Key Pair Generation and Installation 31
6.1.1 Key Pair Generation 31
6.1.2 Subscriber Public Key Delivery 31
6.1.3 Public Key Delivery to Subscriber 31
6.1.4 Key Sizes 31
6.1.5 Standards for Cryptographic Module 31
6.1.6 Key Usage Purposes 31
6.2 Private Key Protection 31
6.2.1 Standards for Cryptographic Module 31
6.2.2 Private Key Multi-Person Control 31

6.2.3 Private Key Escrow 31
6.2.4 Backup of HKPost Private Keys 32
6.3 Other Aspects of Key Pair Management 32
6.4 Computer Security Controls 32
6.5 Life Cycle Technical Security Controls 32
6.6 Network Security Controls 32
6.7 Cryptographic Module Engineering Controls 32
7. CERTIFICATE AND CERTIFICATE REVOCATION LIST PROFILES 33
7.1 Certificate Profile 33
7.2 Certificate Revocation List Profile 33
8. CPS ADMINISTRATION 34
Appendix A - Glossary 35
Appendix B - Hongkong Post e-Cert (Organisational Role) Format 39
Appendix C - Hongkong Post Certificate Revocation Lists (CRLs) and Authority Revocation List (ARL) Format 41
Appendix D - Summary of Hongkong Post e-Cert (Organisational Role) Features 44
Appendix E - List of Registration Authorities and Registration Office for the Hongkong Post e-Cert (Organisational Role), if any 45
Appendix F - List of Subcontractor(s) of Certizen Limited for Hongkong Post e-Cert (Organisational Role) Services, if any 50
Appendix G - Lifespan of CA root certificates 51
Appendix H - List of Subscriber Organisations and the corresponding Designated Applications of Hongkong Post e-Cert (Organisational Role) Certificates 52

© COPYRIGHT of this document is vested in the Postmaster General. This document may not be reproduced in whole or in part without the express permission of the Postmaster General.

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, the 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 July 2023 to 30 June 2026, and an extended period up to 30 June 2027 (date inclusive).

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

HKPost remains a recognized CA under Section 34 of the Ordinance and the Contractor is an agent of HKPost appointed pursuant to Section 3.2 of the Code of Practice for Recognized Certification Authorities issued by the Commissioner for Digital Policy under Section 33 of the Ordinance.

HKPost, as a recognized CA, is responsible under the Ordinance for the use of a Trustworthy System for the issuance, revocation or suspension, and publication in a publicly available Repository of recognized and accepted digital certificates for secure on-line identification. **The certificates issued under this CPS are Recognized Certificates under the Ordinance and are referred to as "Certificates" or "e-Cert (Organisational Role)" 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 Commissioner for Digital Policy, HKPost may appoint agents or subcontractors to carry out some or all of its operations.

This CPS sets out practices and standards for e-Cert (Organisational Role), and the structure of this CPS is as follows:

Section 1 provides an overview and contact details
Section 2 sets out the responsibilities and liabilities of the parties

Section 3 sets out application and identity confirmation procedures
Section 4 describes the operational requirements
Section 5 presents the security controls
Section 6 sets out how the Public/Private Key pairs will be generated and controlled
Section 7 describes the certificate and certificate revocation list profiles
Section 8 documents how this CPS will be administered

Appendix A contains a glossary
Appendix B contains a Hongkong Post e-Cert (Organisational Role) format
Appendix C contains a Hongkong Post Certificate Revocation List (CRL) format
Appendix D contains a summary of Hongkong Post e-Cert (Organisational Role) features
Appendix E contains a list of Hongkong Post e-Cert (Organisational Role) Registration Authorities (RAs), if any
Appendix F contains a list of Subcontractor(s) of Certizen Limited for Hongkong Post e-Cert (Organisational Role) Services, if any
Appendix G describes lifespan of CA root certificates
Appendix H contains a list of Subscriber Organisations and the corresponding Designated Applications of Hongkong Post e-Cert (Organisational Role) Certificates

1. INTRODUCTION

1.1 Overview

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

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**") "**1.3.6.1.4.1.16030.1.3.22**" (see description of the field "Certificate Policies" in **Appendix B**).

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

e-Cert (Organisational Role) 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 the Designated Application of the certificate. Relying Party must not make use of the HKPost issued certificate in any PKI applications other than the Designated Application in respect of the Subscriber Organisation of the certificate listed in **Appendix H**.

Offer of e-Cert (Organisational Role) certificates requires prior arrangement between the subscriber organisation and HKPost before HKPost issues e-Cert (Organisational Role) certificates for that subscriber organisation.

Under the Ordinance, HKPost is a recognized CA. **HKPost has designated the e-Cert (Organisational Role) 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 or suspension, and publication in a publicly available Repository of accepted Recognized Certificates. Recognized Certificates have characteristics of accuracy and contain representations of fact which are defined in law by the Ordinance, including a representation (as further defined below) that such certificates have been issued in accordance with this CPS. The fact that HKPost has appointed agents or contractors or subcontractors does not diminish HKPost's obligation to use a Trustworthy System, nor does it alter the characteristics that e-Cert (Organisational Role) certificates have as recognized certificates.

A summary of the e-Cert (Organisational Role) features is in **Appendix D**.

1.2 Community and Applicability

1.2.1 Certification Authority

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

1.2.1.1 Representations by HKPost

By issuing a certificate that refers to this CPS, HKPost represents to Relying Parties who act in accordance with Section 2.1.5 and other relevant sections of this CPS, that HKPost has issued the certificate in accordance with this CPS. By publishing a certificate that refers to this CPS, HKPost represents to Relying Parties who act in accordance with Section 2.1.5 and other relevant sections of this CPS that HKPost has issued the certificate to the Subscriber identified in it.

1.2.1.2 Effect

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

1.2.1.3 HKPost's Right to Subcontract

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

1.2.2 Registration Authority

The Registration Authority ("RA") is the agent appointed by HKPost or a sub-contractor of the Contractor (and therefore also acting for HKPost) in performing some limited functions such as verification of the identity of the Applicant, and the identity and due authorisation of the Authorised Representative(s) and Authorised User(s) of the Applicant who has submitted application of e-Cert (Organisational Role) (first time or renewal). Similarly, verification of the identity of the Subscriber (and of its Authorised Representative or Authorised User) in the case of any revocation request from such Subscriber. All other functions and obligations, including the functions to be performed by Registration Office arising from the usage from time to time of the e-Cert (Organisational Role), regardless of the nature of the Designated Applications, are functions and obligations undertaken by the Registration Office as agent for its Subscriber but not as sub-contractor or agent for the Contractor and for HKPost.

1.2.3 End Entities

Under this CPS there are two types of end entities, Subscribers and Relying Parties. A Subscriber is the "Subscriber Organisation" referred to in **Appendix A**. Relying Parties are entities that have relied on any class or category of e-Cert (Organisational Role) for use in a transaction of the Designated Application referred to in **Appendix H**. For the avoidance of doubt, Relying Parties should not rely on the Registration Authority or the Contractor. For e-Cert (Organisational Role) certificates that are issued via the Registration Authority or the Contractor, the Registration Authority and the Contractor do not owe a duty of care and are not responsible to the Relying Parties in anyway for the issue of those e-Cert (Organisational Role) certificates (see also Section 2.1.2). Subscribers who rely on an e-Cert (Organisational Role) of another Subscriber for use in a transaction of the Designated Application of the Subscriber Organisation referred to in **Appendix H** will be Relying Parties in respect of such a certificate.

1.2.3.1 Warranties and Representations by Applicants and Subscribers

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

a) Subscriber Organisation warrants that the Authorised User is reminded to safeguard the secrets that is required for accessing the corresponding Private Key stored in HSM of the Registration Office;
b) Subscriber Organisation ensures that no person other than the Authorised User identified in the e-Cert (Organisational Role) can make use of the corresponding Private Key to generate Digital Signature;
c) Each Digital Signature generated using the Private Key of an e-Cert (Organisational Role), which corresponds to the Public Key contained in the e-Cert (Organisational Role), is the Digital Signature of the corresponding Authorised User identified in the e-Cert (Organisational Role);
d) All Information and representations made by the Subscriber Organisation 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;

g) e-Cert (Organisational Role) certificates are to be used only by the Authorised Users and for the Designated Application stipulated in **Appendix H**; and
h) Subscriber Organisation warrants that the Authorised Representative of Subscriber Organisation does not perform the roles and responsibilities of Registration Authority referred to in **Appendix E**;

1.2.3.2 Registration Office
Registration Office of a Subscriber Organisation ("RO") undertakes all functions and obligations arising from the certificate life-cycle management and the usage from time to time of the e-Cert (Organisational Role), regardless of the nature of the Designated Application for its Subscriber. Registration Office is not a sub-contractor of nor an agent for the Contractor or for HKPost.

1.2.4 Classes of Subscribers

HKPost issues certificates under this CPS only to Applicants whose application for a certificate has been approved and confirmed their acceptance of a Subscriber Agreement in the appropriate form.

An e-Cert (Organisational Role) certificate is issued to Bureaux and Departments of the Government of Hong Kong SAR, organisations that hold a valid business registration certificate issued by the Government of the Hong Kong SAR and statutory bodies of Hong Kong SAR whose existence is recognized by the laws of Hong Kong SAR (the "Subscriber Organisation" as listed in **Appendix H**); and identifies a member or employee of a Subscriber Organisation whom that Subscriber Organisation has duly authorised the use of Private Key of that e-Cert (Organisational Role) issued to that Subscriber Organisation (the "Authorised User"). Offer of e-Cert (Organisational Role) certificates requires prior arrangement between HKPost and the Subscriber Organisation.

e-Cert (Organisational Role) certificates can only be used by Authorised Users in respect of the Designated Applications set out against the name of that Subscriber Organisation referred to in **Appendix H**.

SUBSCRIBER ORGANISATION UNDERTAKES TO HKPOST NOT TO GIVE AUTHORITY TO THE AUTHORISED USER OF THE E-CERT (ORGANISATIONAL ROLE) TO USE THE CERTIFICATE FOR ANY PURPOSE OTHER THAN TO ENCRYPT AND DECRYPT ELECTRONIC MESSAGES, OR GENERATE A DIGITAL SIGNATURE WITHIN THE DESIGNATED APPLICATION REFERRED TO IN **APPENDIX H**.

1.2.4.1 e-Cert (Organisational Role) Certificate

There is only one class of e-Cert (Organisational Role) issued under this CPS.

1.2.5 Certificate Lifespan

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

Certificates issued under this CPS may have different lifespans depending upon the Subscriber Organisation in connection with which certificate. HKPost will agree with that Subscriber Organisation the length of validity applicable to the e-Cert (Organisational Role) in relation to which that Subscriber Organisation will act. The lifespan of certificates is set out in **Appendix H.** (See Section 3.2 for Certificate Renewal).

1.2.6 Application at Premises Designated by HKPost
All first applications and applications of a new e-Cert (Organisational Role) following the revocation or expiration of e-Cert (Organisational Role) will require the Applicants (represented by Authorised Representative) to submit their applications as described in sections 3 and 4 of this CPS.

1.3 Contact Details

Subscribers may send their enquiries, suggestions or complaints by:

Mail to : Hongkong Post Certification Authority, Kowloon East Post Office Box 68777
Tel: 2921 6633
Fax: 2775 9130
Email: enquiry@eCert.gov.hk

1.4 Complaints Handling Procedures

HKPost will handle all written and verbal complaints expeditiously. Upon receipt of the complaint, a full reply will be given to the complainant within 7 working days. In the cases where full replies cannot be issued within 7 working days, interim replies will be issued. As soon as practicable, designated staff of HKPost will contact the complainants by phone, email or letter mail to acknowledge and reply to the complaints.

2. GENERAL PROVISIONS

2.1 Obligations

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

2.1.1 CA Obligations

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

a) receive application for certificates via a Registration Authority;
b) process application for certificates via a Registration Authority;
c) issue and publish certificates in a timely manner (see Section 2.5);
d) notify Applicants, via a Registration Authority, approval or rejection of their applications (see Section 4.1);
e) suspend or revoke certificates and publish Certificate Revocation Lists in a timely manner (see Section 4.4); and
f) notify Subscribers, whether via Registration Authority or directly, of the suspension or revocation of their certificates (see Sections 4.4.1, 4.4.2 and 4.4.3).

2.1.2 Registration Authority Obligations

Registration Authority is responsible for:

a) receiving certificate applications from the Authorised Representative of the Applicant;
b) verifying the identity of the Applicant and also the identity and due authorisation of the Authorised Representative(s) and Authorised User(s) of the Applicant, both in first time application and renewal of e-Cert (Organisational Role); verifying the identity of the Subscriber and also the identity of the Authorised Representative(s) or Authorised User(s), in any request for revocation of e-Cert (Organisational Role);
c) retention of documentary evidence that identifies the Applicants and Subscribers;
d) submitting certificate requests received from the Authorised Representative of the Applicant to HKPost; and
e) receiving notification of approval or rejection of the Applicant's application on behalf of the Applicant, and conveying such notification to the Applicant.

Registration Authorities (RAs) under this CPS if any as listed in **Appendix E** are appointed by Certizen Limited as its Subcontractor to perform part of the Contract as detailed in this CPS.

The persons or members of the Registration Authority nominated to perform the roles and responsibilities of the Registration Authority referred to in **Appendix E** shall not be Authorised Representative of Subscriber Organisations to apply for e-Cert (Organisational Role) certificate and shall not perform the roles and responsibilities of Registration Office.

The Registration Authority acknowledges that if it does not discharge the above duties properly or at all, it become liable under the sub-contract with Certizen Limited, and/or, under the law, to pay the Government (acting through the HKPCA), or other persons (including Relying Parties), damages in respect of liabilities or loss and damage they may incur or suffer in consequence.

2.1.3 Contractor Obligations

The Contractor is responsible only to HKPost under the terms of the Contract between HKPost and the Contractor under which the Contractor has been appointed by HKPost as its agent to

set up, modify, provide, supply, deliver, operate, administer, promote and maintain the HKPost CA systems and services as stipulated in this CPS. HKPost is and remains responsible for the activities of the Contractor in the performance or purported performance by the Contractor of the functions, power, rights and duties of HKPost.

2.1.4 Registration Office Obligations

Registration Office is responsible for:

a) Sending application request to Registration Authority for identity verification by a Authorised Representative appointed by Registration Office;
b) Submitting certificate signing requests on behalf of the Applicant to Registration Authority containing information in relation to the Applicant and its Authorised Representative(s) and Authorised User(s) that matches with the information known to the Registration Office at time of submission, together with a confirmation of subscriber terms and conditions specified in the application form entered between the Applicant and HKPost;
c) When applications are approved by HKPost and certificates are issued, on behalf of the Applicant, accepting the issued e-Cert (Organisational Role) from HKPost in a secure manner;
d) Quoting the Applicant/Subscriber's information through the use of a unique identity number assigned, which must uniquely refer to the Subscriber's evidence of identity, for submission of e-Cert (Organisational Role) application;
e) Ensuring that the generation of the Subscriber's Key Pair and its storage only in a Hardware Security Module of the Registration Office;
f) Ensuring the safe custody of the Subscriber's Key Pair;
g) Ensuring that for e-Cert (Organisational Role), it is used for the corresponding Designated Application specified opposite its name in **Appendix H** only;
h) Ensuring that the use by a Subscriber of a e-Cert (Organisational Role) for purposes other than the Designated Application referred to in **Appendix H** specified opposite its name will not be permitted;
i) Ensuring that only the corresponding Authorised User specified in the e-Cert (Organisational Role) can make use of his/her Private Key to generate digital signature for the relevant Designated Application;
j) Verifying the identity of the Authorised User of the Subscriber, before the Authorised User is permitted using its e-Cert (Organisational Role) in Designated Application;
k) In each time an e-Cert (Organisational Role) issued is used in a Designated Transaction, ensuring that the e-Cert (Organisational Role) has not expired or revoked or suspended based on the information as shown in the Repository and the CRL. Where e-Cert (Organisational Role) has expired or has been revoked or suspended, ensuring that the Designated Application will not be processed or completed using such e-Cert (Organisational Role);
l) Complying with all notices, instructions and manuals issued by HKPost from time to time; and
m) Complying with this CPS.

2.1.5 Subscriber Obligations

Subscribers are responsible for:

a) Agreeing that the key pair is generated by Registration Office in a Hardware Security Module and environment within Registration Office's premises on behalf of the Subscriber.
b) Completing the application procedures properly and 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.
c) authorising the Registration Office to perform tasks mentioned in Section 2.1.4 above.
d) Accurately following the procedures specified in this CPS as to the expiry of Certificates.
e) Notifying the Registration Authority identified in the relevant certificate immediately from time to time of any change in the Information in the certificate provided by the Subscriber or of any change in the Authorised User such as change of Role of the Authorised User.
f) Notifying the Registration Authority identified in the relevant certificate immediately from

time to time of any change in the appointment and information of the Authorised Representative.

g) Notifying the Registration Authority identified in the relevant certificate immediately of any fact which may give rise to HKPost, upon the grounds set out in Section 4 below, having the right to revoke the certificate for which that Subscriber is responsible.

h) Agreeing that by having been issued or accepting a certificate they warrant (promise) to HKPost and represent to all Relying Parties that during the operational period of the certificate, the facts stated in Section 1.2.3.1 above are and will remain true.

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

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

k) Acknowledging that by submitting an e-Cert (Organisational Role) application, they authorise the publication of the e-Cert (Organisational Role) to any other person or in the HKPost's Repository.

2.1.5.1 Subscriber's Liability

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

2.1.6 Relying Party Obligations

Relying Parties relying upon e-Cert (Organisational Role) 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 an e-Cert (Organisational Role) certificate determining that the use of the e-Cert (Organisational Role) certificate is appropriate for its purposes in the corresponding Designated Application under this CPS while the Contractor or Registration Authority (if any, see **Appendix E and F**) does not undertake any duty of care to Relying Parties at all.

c) Acknowledging that HKPost, the Registration Authority or the Contractor does not undertake any responsibility or duty of care to Relying Parties if the e-Cert (Organisational Role) certificate is used or relied upon for any purposes other than the Designated Application of the respective Subscriber Organisation referred to in **Appendix H** of this CPS.

d) Checking the status of the certificate on the certificate revocation list prior to reliance.

e) Performing all appropriate certificate path validation procedures.

2.2 Further Provisions

Obligations of HKPost to Subscribers and Relying Parties

2.2.1 Reasonable Skill and Care

As the Subscriber is also at the same time the Registration Authority, HKPost does not undertake to the Subscriber or any Relying Party that a reasonable degree of skill and care will be exercised by HKPost, by the Contractor and by the Registration Authority when acting on its behalf 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. HKPost does not warrant that the services it provides under this CPS by itself, by the Contractor or by the Registration Authority or otherwise howsoever will be uninterrupted or error free or of a higher or different standard than that which should be achieved by HKPost, or the officers, employees or agents of Hong Kong Post Office.

The implications of this are that 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 Registration Authority are under no liability of any kind in respect of such liability, loss or damage.

This means, HKPost, Hong Kong Post Office, the Contractor and any such Registration Authority will not be liable for any loss to a Subscriber or Relying Party caused by their reliance upon a false or forged Digital Signature or authorisation of person as Authorised Representative or Authorised User of the Subscriber's e-Cert (Organisational Role) who should not have been authorised.

This means, also, that, neither HKPost, the Hong Kong Post Office, the Contractor nor any such Registration Authority is liable for the adverse effects to Subscribers or Relying Parties of any matters outside HKPost's control whatsoever, including (without limitation) the availability of the Internet, or telecommunications or other infrastructure systems or the adverse effects of the acts of God, war, military operations, national emergency, epidemic, fire, flood, earthquake, strike or riots or the negligence or deliberate wrongful conduct of other Subscribers or other third parties.

2.2.2 No Supply of Goods

For the avoidance of doubt, a Subscriber Agreement is not a contract for the supply of goods of any description or at all. Any and all certificates issued pursuant to it remain the property of and in the possession and control of HKPost and no right, title or interest in the certificates is transferred to the Subscriber, who merely has the right to procure the issue of a certificate and to rely upon it and the certificates of other Subscribers in accordance with the terms of the Subscriber Agreements. Accordingly, the Subscriber Agreements contain (or are to contain) no express or implied terms or warranties as to the merchantability or fitness of a certificate for a particular purpose or any other terms or conditions appropriate in a contract for the supply of goods. Equally HKPost, in making available the certificates in a public Repository accessible by Relying Parties is not supplying any goods to Relying Parties and likewise gives to Relying Parties no warranty as to the merchantability or fitness for a particular purpose of a certificate nor makes any other representation or warranty as if it were supplying goods to Relying Parties. HKPost agrees to transfer those articles into possession of Applicants or Subscribers for the limited purposes set out in this CPS. Nonetheless HKPost will exercise reasonable care to see that the same is fit for the purposes of completing and accepting a certificate as set out in this CPS, and if it is not, then HKPost's liability shall be as set out in sections 2.2.3 - 2.2.4 below. In addition, the articles transferred from HKPost may contain other material not relevant to the completion and acceptance of an e-Cert (Organisational Role) and if it does, the legal position in relation to such material is not governed by the CPS or the Subscriber Agreement, but by separate terms and conditions that will be referred to in the terms and conditions enclosed in the articles.

2.2.3 Limitation of Liability

2.2.3.1 Reasonableness of Limitations

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

2.2.3.2 Limitation on Types of Recoverable Loss

In the event of HKPost's breach of :-
a) the Subscriber Agreement;

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

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

2.2.3.3 HK$15,000 Limit
Subject to the exceptions that appear below, in the event of HKPost's breach of:-

a) the Subscriber Agreement and provision of this CPS; or
b) any duty of care, and in particular, any duty under the Subscriber Agreement, under this CPS or in law to exercise reasonable skill and care (but there is no provision (express or implied) imposing on HKPost any duty to exercise reasonable skill and care under this CPS or in the Subscriber Agreement) 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 $15,000 in respect of one e-Cert (Organisational Role) certificate.

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

2.2.3.5 Hong Kong Post Office, the Contractor, RAs and their Personnel
Neither the Hong Kong Post Office, the Contractor nor any Registration Authority nor any officer or employee or other agent of the Hong Kong Post Office, the Contractor, or any Registration Authority 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 Registration Authority nor any of their respective officers, employees or agents voluntarily accepts or will accept any personal responsibility or duty of care to the Subscriber or Relying Parties in connection with any action or omission done in good faith by any of them in any way connected either with the performance of HKPost of a Subscriber Agreement or any certificate issued by HKPost as a CA and each and every Subscriber and Relying Party accepts and will continue to accept that and undertakes to HKPost not to sue or seek any form of recovery or redress by other legal means whatsoever from any of the foregoing in respect of any act or omission done by that person in good faith (whether done negligently or not) in any way connected with either the performance of HKPost of a Subscriber Agreement or any certificate issued

by HKPost as a CA and acknowledges that HKPost has a sufficient legal and financial interest to protect these organisations and individuals from such actions.

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

2.2.3.7 Certificate Notices, Limitations and Reliance Limit
e-Cert (Organisational Role) 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-Cert (Organisational Role) certificates which may be read on the HKPost CA web site at http://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.*
>
> *The Postmaster General (by the Hong Kong Post Office, the Contractor, and their respective officers, employees and agents including, without limitation, the Registration Authority) issues this certificate without undertaking any responsibility or duty of care to Relying Parties.*
>
> *Relying Parties, before relying upon this certificate are responsible for:-*
> *a) Relying on it only when reliance is reasonable and in good faith in the light of all the circumstances known to the Relying Party at the time of reliance;*
> *b) Before relying upon this certificate, determining that the use of the certificate is appropriate for its purposes in corresponding Designated Applications under the CPS;*
> *c) Acknowledging that the Postmaster General, Hong Kong Post Office, the Contractor, any Registration Authority and their respective officers, employees or agents do not undertake any responsibility or duty of care to Relying Parties.*
> *d) Checking the status of this certificate on the Certificate Revocation List prior to reliance; and*
> *e) Performing all appropriate certificate path validation procedures.*
>
> *If the Contractor, any Registration Authority 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, any Registration Authority 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, any Registration Authority or their respective officers, employees or agents, then the Postmaster General will pay a Relying Party up to HK$15,000 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$15,000 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, any Registration Authority 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, suspension, revocation or publication of this e-Cert (Organisational Role) 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, any Registration Authority and their officers, employees or agents, this certificate does not impose any limit upon their liability to Relying Parties who suffer loss in consequence of reasonable reliance upon such misrepresentations in this certificate.

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

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

2.2.5 Assignment by Subscriber
Subscribers shall not assign their rights under Subscriber Agreement or Certificates. Any attempted assignment will be void.

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

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

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

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

2.2.10 Fiduciary Relationships
None of HKPost, the Contractor nor any Registration Authority 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 Registration Authority, by contract or otherwise, to any obligation as an agent, fiduciary, trustee or other representative of the Subscribers or Relying Parties. In particular, Authorised Representative of the Subscribers must not act as member of Registration Authority; and member of Registration Authority must not act as Authorised Representative of the Subscribers.

2.2.11 Cross Certification
HKPost reserves the right in all instances to define and determine suitable grounds for cross-certification with another CA.

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

2.3 Interpretation and Enforcement (Governing Law)

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

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

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

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

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

2.4 Subscription Fees

The subscription fee and administration fee shall be paid by e-Cert (Organisational Role) subscribers unless waived by HKPost. For details of the fees charged in respect of e-Cert (Organisational Role) certificates, please see **Appendix H** under the heading of the relevant Subscriber Organisation. 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 fees as specified in **Appendix H** from e-Cert (Organisational Role) subscribers.

2.5 Publication and Repository

Under the Ordinance, HKPost maintains a Repository that contains a list of accepted certificates

issued under this CPS, the current certificate revocation list, the HKPost Public Key, a copy of this CPS, and other Information related to e-Cert (Organisational Role) certificates which reference this CPS. The Repository is available on a substantially 24 hours per day, 7 days per week basis, subject to scheduled maintenance of an average of 2 hours per week and any emergency maintenance. HKPost promptly publishes each certificate accepted by and issued to the Subscriber under this CPS in the Repository. The HKPost Repository can be accessed at URLs as follows:-

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

or alternatively

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

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

2.5.2 Certificate Repository Access Requirements
Only persons authorised by HKPost have access to the Repository to update and modify the contents.

2.5.3 Certificate Repository Update Cycle
The Repository is updated promptly after each certificate is accepted by and issued to the Subscriber and any other applicable events such as update of certificate revocation list.

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

2.6 Compliance Assessment

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

2.7 Confidentiality

HKPost will 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 or suspending and publishing e-Cert (Organisational Role) certificates shall not disclose or permit or suffer to be disclosed any information relating to another person as contained in such record, book, register, correspondence, information, document or other material to any other person. Information about Subscribers that is submitted as part of an application for an e-Cert (Organisational Role) certificate under this CPS will be used only for the purposes collected and is kept confidential except to the extent necessary for HKPost, the Contractor or RAs to perform HKPost's obligations under this CPS. Such Information will not be released without the prior consent of the Subscriber except when required by a court-issued subpoena or order, or when otherwise required by the laws of Hong Kong SAR. HKPost is specifically precluded from releasing lists of Subscribers or Subscriber Information (except for the release of compiled data which is not traceable to an individual Subscriber) unless required by a court-issued subpoena or order, or when otherwise required by the laws of Hong Kong SAR.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Initial Application

The Authorised Representative, who is appointed by Registration Office, must appear in person at a designated HKPost premises, or premises of the Registration Authority designated by HKPost, and present proof of identity as described in section 3.1.8. Attendance of Authorised Users who will be identified in e-Cert (Organisational Role) is not required.

All Applicants for e-Cert (Organisational Role) shall submit requests for certificate electronically. e-Cert (Organisational Role) certificate application requires the Authorised Representative of the Organisation to submit certificate signing request for e-Cert (Organisational Role) and the Organisation will become a Subscriber. Following approval of the application, HKPost will prepare an e-Cert (Organisational Role) and notifies the Applicant of how the Certificate may be issued.

3.1.1 Types of Names

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

a) The Authorised User's identifier and/or name as it appears on the documents to verify its identity as specified in **Appendix H** against the Subscriber Organisation;
b) The Subscriber Organisation's name as it is registered with the appropriate Hong Kong Government Department or registration agency or as a statutory body whose existence is recognized by the laws of Hong Kong SAR, or the official name of that Bureau or Department where the Subscriber Organisation is a Bureau or Department of the Government of Hong Kong SAR; and
c) 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 as a statutory body whose existence is recognized by the laws of Hong Kong SAR.

3.1.1.2 The Authorised Representative
Although the Authorised Representative of the Subscriber Organisation, who is appointed by Registration Office, is responsible for administering on behalf of the Subscriber Organisation the application for an e-Cert (Organisational Role) certificate, that person will not be identified in the e-Cert (Organisational Role) certificate.

3.1.1.3 Organisation Names in Chinese Language
All e-Cert (Organisational Role) certificates are issued in English language only. For organisations who subscribe to e-Cert (Organisational Role) and are companies with company names in the Chinese language only or who have provided their company's Chinese name only, their company names will not be displayed in the e-Cert (Organisational Role).

3.1.2 Need for Names to be Meaningful
All names must be meaningful using commonly understood semantics to determine the identity of the Subscriber.

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

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

3.1.5 Name Claim Dispute Resolution Procedure

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

3.1.6 Infringement and Violation of Trademarks

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

3.1.7 Method to Prove Possession of the Private Key

Registration Office shall carry out the key generation service on behalf of the Subscriber in a Hardware Security Module hosted in a Trustworthy System and environment within the Registration Office's premises to ensure that the Private Key is not tampered with, and shall generate and transmit the Certificate Signing Request (CSR) containing the Public Key to HKPost. HKPost will generate the Certificate within HKPost's premises. The issued Certificate in which the Applicant's Public Key is included will be delivered to the Applicant via Registration Office, in a secure manner stipulated in Section 4.2 below.

3.1.8 Authentication of Identity of Organisational Applicant

3.1.8.1 Applications for e-Cert (Organisational Role) certificates should be made at a designated HKPost premises, or premises of the Registration Authority designated by HKPost by the personal attendance of the Applicant's Authorised Representative who is required to present his/her own HKID Card or passport. At the sole discretion of HKPost, it may be permitted for submission of the application accompanied by a copy of the Authorised Representative's own HKID Card or passport with the Authorised Representative's signature, in lieu of the Authorised Representative's personal attendance, provided that (a) the Authorised Representative's identity has been authenticated in a past application of the Subscriber Organisation, and the Authorised Representative has appeared at a designated HKPost premises, or premises of the Registration Authority designated by HKPost for identity verification in that application; and (b) reasonable justification is available for re-affirming the identity of the Authorised Representative, such as confirmation with the Authorised Representative through telephone call or checking the Authorised Representative's signature against that on past application records. In case of doubt, HKPost may decline the application.

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

a) an authorisation letter, bearing the "For and on behalf of" chop (if applicable) and the authorised signature(s) of the organisation giving authority to the Authorised Representative to make the application;
b) documentation to verify the identity of each Authorised User, where documentation means either a photocopy of the HKID Card, or a photocopy of a valid travel document if the Authorised User is not a Hong Kong citizen, or the documents containing the documentary evidence, e.g. HKID Card or passport information, as to be usable for subsequent reference to verify the identity of the Authorised User of the respective Subscriber Organisation referred in **Appendix H**;
c) documentation issued by the appropriate Hong Kong registration agency attesting to the existence of the organisation. The validity of the documentation should not expire within two months by the time the application is submitted.

3.1.8.3 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, if applicable) appointing the Authorised Representative to submit on behalf of the Bureau or Department, any documents relating to the application, revocation and renewal of HKPost e-Cert (Organisational Role) certificates. The memo, letter or relevant application form must be signed by a Departmental Secretary or officer at equivalent level or above.

3.2 Certificate Renewal

3.2.1 e-Cert (Organisational Role) certificates

HKPost will notify Subscribers to renew the e-Cert (Organisational Role) 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 will not perform renewal of expired, suspended or revoked certificates.

There is no automatic renewal of an e-Cert (Organisational Role) certificate. The Authorised Representative of the Subscriber Organisation will need to submit the renewal request electronically via Registration Office to HKPost and pay for appropriate subscription fees. The process of "Authentication of identity of Organisational Applicant" as described under Section 3.1.8 will be conducted as if a new application is received. In circumstances where Authorised Representatives are replaced, the new Authorised Representative will need to also complete and submit an authorisation document as described under Section 3.1.8.2(a) or 3.1.8.3.

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

3.2.2 Validity Period of Renewed e-Cert (Organisational Role)

At the discretion of HKPost, the new e-Cert (Organisational Role) certificate to be issued to the Subscriber may be valid as from the date the new certificate is generated and expired on the date that is the new certificate lifespan after the expiry date of the old certificate being renewed. Accordingly, the new e-Cert (Organisational Role) certificate may have a validity period of more than the certificate lifespan specified in Section 1.2.5 but no more than such certificate lifespan and two months.

4. OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Applicants for e-Cert (Organisational Role) certificates under this CPS must complete and submit an application electronically via Registration Office to the Registration Authority designated by HKPost. The Registration Authority shall complete and transmit the application to the HKPost.

4.1.2 By submitting an e-Cert (Organisational Role) request electronically via Registration Office, the Applicant authorises the publication of the e-Cert (Organisational Role) to any other person or in the Repository and accepts the e-Cert (Organisational Role) to be issued to the Applicant.

4.1.3 The documentation required for proving the identity of the Applicant is stipulated in Section 3.1.8 (Authentication of Identity of Organisational Applicant) of this CPS. HKPost, or the Registration Authority, will verify the identity of the Authorised Representative.

4.2 Certificate Issuance

4.2.1 Following the identity verification process, Registration Office shall carry out the central key generation service on behalf of the Subscriber in a Hardware Security Module hosted in a Trustworthy System and environment within the Registration Office's premises to ensure that the Private Key is not tampered with, and shall generate and transmit the Certificate Signing Request (CSR) containing the Public Key to HKPost. HKPost will generate the e-Cert (Organisational Role) certificates (with the Public Key included) of the respective Authorised Users in a Trustworthy System and environment within HKPost's premises.

4.2.2 The e-Cert (Organisational Role) will then be delivered electronically to the Authorised Representative via Registration Office.

4.2.3 The Subscriber Organisation agrees that it is fully accountable for the safe custody of the Private Key upon receipt of the e-Cert (Organisational Role) certificate and agree that they will be responsible for any consequences under any circumstances for the compromise of the Private Key.

4.2.4 All Private Keys stored in the HSM hosted in a Trustworthy System and environment within the Registration Office's premises are in an encrypted form. Proper security controls are in place to guard against unauthorised access to and disclosure of the encrypted Private Keys.

4.3 Publication of e-Cert (Organisational Role)

Under the Ordinance, HKPost's system will promptly publish the accepted and issued e-Cert (Organisational Role) in the Repository (see Section 2.5). Applicants can either verify the information on the Certificate by browsing the Certificate file or through HKPost CA Repository. Subscriber Organisations should notify HKPost immediately of any incorrect information of the Certificate.

4.4 Certificate Suspension and Revocation

4.4.1 Circumstances for Suspension and Revocation

The compromise of a HKPost Private Key will result in prompt revocation of the certificates issued under that Private Key. Procedures stipulated in the HKPost key compromise plan will be exercised to facilitate rapid revocation of all Subscriber certificates in the event of compromise of the HKPost Private Keys (see Section 4.8.2).

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

Each Subscriber **MUST** apply to either HKPost directly or to the Registration Authority 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 (Organisational Role) has been, or is suspected of having been, compromised or any change in the Information in the certificate provided by the Subscriber or the Role of the Authorised User in the corresponding e-Cert (Organisational Role) is changed or becomes invalid (see also Section 2.1.5(f)).**

HKPost and the Registration Authority, on behalf of HKPost, may suspend or revoke a certificate and will notify the Subscriber by updating the certificate revocation list and by email, if a contact email address is available, of such suspension or revocation ("Notice of Revocation") in accordance with the procedures in the CPS whenever it:-

a) knows or reasonably suspects that a Subscriber's Private Key has been compromised;
b) knows or reasonably suspects that any details upon a certificate are not true or have become untrue or that the certificate is otherwise unreliable;
c) determines that a certificate was not properly issued in accordance with the CPS;
d) determines that the Subscriber had failed to meet any of the obligations set out in this CPS or the Subscriber Agreement;
e) is required to do so by any regulation, or law applicable to the certificate;
f) determines that the Subscriber has failed to pay the subscription fee;
g) knows or has reasonable cause to believe that the Authorised User identified in an e-Cert (Organisational Role) certificate has ceased to be an Authorised User of the Subscriber Organisation;
h) knows or has reasonable cause to believe that the Authorised User identified in an e-Cert (Organisational Role) certificate has ceased to possess the Role in the Subscriber Organisation;
i) knows or has reasonable cause to believe that the Subscriber or Authorised User whose details appear on the e-Cert (Organisational Role) certificate that:-

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

4.4.2 Revocation Request Procedure

An Authorised User, or the Authorised Representative of a Subscriber Organisation, may submit a certificate revocation request directly to HKPost through a designated web page on the HKPost web site at http://www.eCert.gov.hk, by fax, letter mail, email or in-person, or electronically through the Registration Authority which will forward such certificate revocation requests electronically to HKPost.

For certificate revocation request submitted directly to HKPost, HKPost will suspend the validity of the certificate first. The certificate will be revoked, which terminates the validity of the certificate permanently, upon receipt of the final confirmation of revocation from the Authorised User or the Authorised Representative of a Subscriber Organisation or through the Registration Authority to which the request for revocation was first submitted. Such final confirmation of

revocation can be an email digitally signed by the Authorised User's Private Key, or a Request for Certificate Revocation Form signed by the Authorised User or the Authorised Representative of the Subscriber Organisation. If no final confirmation of revocation is received from the Authorised User or the Authorised Representative of the Subscriber Organisation, the validity of the certificate will remain suspended and will be included in the Certificate Revocation List (CRL) until the certificate expires. The Request for Certificate Revocation Form can be obtained from the web site at http://www.eCert.gov.hk or from the Registration Authority (see **Appendix E**). HKPost may consider Authorised User's request or Authorised Representative's request for resuming the validity of certificates that are suspended. However, resuming the validity of a certificate that is suspended is only at the discretion of HKPost.

For certificate revocation request submitted through the Registration Authority to HKPost, HKPost will revoke the certificate so that the validity of the certificate is terminated permanently.

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

Where a revocation request or final confirmation of revocation has been submitted to a Registration Authority, that Registration Authority will, within one working day of receipt, notify HKPost of the receipt of the same to enable HKPost to post the suspension or revocation to the Certificate Revocation List.

Requests for revocation and confirmation of revocation can only be actioned by Registration Authority and HKPost within their usual business hours. For details of the Registration Authority's business hours for accepting requests for revocation, please refer to **Appendix E**.

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.

4.4.3 Service Pledge & Certificate Revocation List Update

a) HKPost will exercise reasonable endeavours to ensure that within 2 working days of (1) receiving a revocation request or final confirmation of revocation from either the Subscriber directly or from the Registration Authority or (2) in the absence of such a request, the decision by HKPost or the notification from a Registration Authority of a decision by that Registration Authority on HKPost's behalf, to suspend or revoke the certificate, the suspension or 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 suspension or revocation. Only when the next Certificate Revocation List is updated and published will it reflect the suspended or revoked status of the certificate. Certificate Revocation Lists are published daily and are archived for at least 7 years.

   For the avoidance of doubt, all Saturdays, Sundays, public holidays and for all weekdays on which a tropical cyclone and rainstorm warning signal is hoisted, are not working days for the purpose of this section 4.4.3(a).

HKPost will exercise reasonable endeavours to notify relevant Subscribers by updating the certificate revocation list and by email, if a contact email address is available, within two working days following the suspension or revocation.

b) Subscribers must not use a certificate in a transaction on becoming aware of any ground upon which HKPost or the Registration Authority 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 of the intention of HKPost or the Registration Authority to suspend or revoke the certificate. HKPost and the Registration Authority shall be under no liability to Subscribers or Relying Parties in respect of any such transactions if, despite the foregoing of this sub-section, they do use the certificate in a transaction.

c) Further, upon becoming so aware of any ground upon which HKPost or the Registration Authority could revoke the certificate, or upon making a revocation request or upon being notified by HKPost or the Registration Authority 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, the Registration Authority or the Contractor 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 and the Registration Authority 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 and the Registration Authority shall be under no liability to Relying Parties in respect of the transactions in the period between HKPost's or the Registration Authority's decision to suspend or revoke a certificate (either in response to a request or otherwise) and the appearance of the suspension or revocation status on the Certificate Revocation List. Any such liability is limited as set out elsewhere in this CPS. In no circumstances does the Registration Authority itself undertake a separate duty of care to Relying Parties (the Registration Authority are simply discharging HKPost's duty of care), and accordingly, even if negligent, the Registration Authority itself cannot be held liable to Relying Parties.

d) The Certificate Revocation List (CRL) is updated and published in accordance with the schedule and format specified in **Appendix C**.

e) HKPost's policy concerning the situation where a Relying Party is temporarily unable to obtain Information on suspended or revoked certificate is stipulated in Section 2.1.5 (Relying Parties Obligations) and Section 2.2.1 (Reasonable Skill and Care) of this CPS.

4.4.4 Effect of Revocation
Revocation terminates a certificate as of the time that HKPost posts the suspension/revocation status to the Certificate Revocation List.

4.5 Computer Security Audit Procedures

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

- Suspicious network activity
- Repeated failed access attempts
- Events related to equipment and software installation, modification, and configuration of the CA operation
- Privileged accesses to all CA components
- Regular certificate management operations including: -
  - Certificate revocation and suspension requests

- Actual issuance, revocation and suspension of certificates
- Certificate renewals
- Updates to repositories
- CRL generation and posting
- CA Key rollover
- Backups
- Emergency key recoveries

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

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

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

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

4.5.6 Audit Information Collection System
HKPost CA audit records and files are under the control of an automated audit collection system that cannot be modified by any application, program, or other system function. Any modification to the audit collection system is itself an auditable event.

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

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

4.6 Records Archival

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

- System equipment configuration files;
- Results of assessments and/or review for accreditation of the equipment (if conducted);
- Certification Practice Statement and its modifications or updates;
- Contractual agreements to which HKPost is bound;
- All certificates and CRLs as issued or published;
- Periodic event logs; and
- Other data necessary for verifying archive contents.

4.6.2 Archive Retention Period
Key and certificate Information is securely maintained for at least 7 years. Audit trail files are maintained in the CA systems as deemed appropriate by HKPost.

4.6.3 Archive Protection
Archived media maintained by HKPost is protected from unauthorised access by various physical and cryptographic means. Protective measures are used to protect the archiving

media from environmental threats such as temperature, humidity and magnetism.

4.6.4 Archive Backup Procedures
Backup copies of the archives will be created and maintained when necessary.

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

4.7 Key Changeover

The lifespan of the HKPost CA and signing root key and certificates created by HKPost (See **Appendix G**) 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 4.6.2 for verification of any signatures generated by the original root keys.

4.8 Disaster Recovery and Key Compromise Plans

4.8.1 Disaster Recovery Plan
A managed process, including daily backup of essential business information and CA system data and proper backup of CA system software, is in place for maintaining business continuity plans to protect critical business processes from the effect of major failures or disasters. Business continuity plans exist to enable the complete recovery of all HKPost 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 exercised annually.

HKPost will promptly notify the Commissioner for Digital Policy and make public announcement of the switchover of operation from the production site to the disaster recovery site as a result of major failures or disasters.

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

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

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

HKPost will promptly notify the Commissioner for Digital Policy and make public announcement if a HKPost Private Key for the issuance of e-Cert (Organisational Role) certificates under this CPS has been compromised. The compromise of a HKPost Private Key will result in prompt revocation of the certificates issued under that Private Key and the issuance of new and replacement certificates.

4.8.3 Key Replacement
In the event of key compromise or disaster where a HKPost Private Key for the issuance of e-Cert (Organisational Role) certificates under this CPS has been compromised or corrupted and cannot be recovered, HKPost will promptly notify the Commissioner for Digital Policy 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 re-issued with new certificates.

4.9 CA Termination

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

4.10 Registration Authority Termination

In the event that the Registration Authority is terminated by Certizen Limited or under CA termination (see Section 4.9) or the Registration Authority's authority is withdrawn, the e-Cert (Organisational Role) certificates applied through the Registration Authority will remain in effect in accordance with their terms and validity.

5. PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY CONTROLS

5.1 Physical Security

5.1.1 Site Location and Construction
The HKPost CA operation is located in a site that affords commercially reasonable physical security. During construction of the site, HKPost took appropriate precautions to prepare the site for CA operations.

5.1.2 Access Controls
HKPost has implemented commercially reasonable physical security controls that limit access to the hardware and software (including the CA server, workstations, and any external cryptographic hardware modules or tokens under HKPost's control) used in connection with providing the HKPost CA services. Access to such hardware and software is limited to those personnel performing in a trusted role as described in Section 5.2.1 of this CPS. Access is controlled and manually or electronically monitored for unauthorised intrusion at all times.

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

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

5.1.5 Fire Prevention and Protection
The CA facility has a fire prevention plan and suppression system in place.

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

5.1.7 Off-site Backup
Adequate backups of the HKPost CA system data will be stored off-site and are afforded adequate protection against theft, destruction and media degradation (See also Section 4.8.1)

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

5.2 Procedural Controls

5.2.1 Trusted Role
Employees, contractors, and consultants of HKPost, of the Contractor and of RAs (collectively "Personnel") that have access to or control of cryptographic or other operations that may materially affect the issuance, use, or revocation of certificates, including access to restricted operations of HKPost's CA database, are considered to be serving in a trusted role. Such Personnel include, but are not limited to, system administration personnel, operators, engineering personnel, and executives who are assigned to oversee HKPost's CA operation.

Procedures are established, documented and implemented for all trusted roles in relation to HKPost e-Cert (Organisational Role) services. The procedural integrity is maintained by enforcing:

- different levels of physical and systems access control based on role and responsibility, and
- segregation of duties.

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

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

5.3 Personnel Controls

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

5.3.2 Background Investigation
HKPost conducts and/or requires the Contractor and RAs to conduct investigations of personnel who serve in trusted roles (prior to their employment and periodically thereafter as necessary) to verify such employees' trustworthiness and competence in accordance with the requirements of this CPS. Personnel who fail an initial or periodic investigation are not permitted to serve or to continue to serve in a trusted role.

5.3.3 Training Requirements
HKPost personnel and those of the Contractor's and of Registration Authority's have received the initial training needed to perform their duties. HKPost and the Contractor also provide ongoing training as necessary to enable their respective personnel to remain current in required skills.

5.3.4 Documentation Supplied To Personnel
HKPost personnel and those of the Contractor's and of Registration Authority's receive comprehensive user manuals detailing the procedures for certificate creation, issuance, updating, renewal, and revocation, and other software functionality relative to their role.

6. TECHNICAL SECURITY CONTROLS

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

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation
Key pairs for HKPost 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.

Key pairs for Applicants/Subscribers are generated in a Hardware Security Module hosted in a Trustworthy System and environment within the Registration Office's premises to ensure that the Private Key is not tampered with.

6.1.2 Subscriber Public Key Delivery
Key pairs for e-Cert (Organisational Role) will be generated under the HSM by Registration Office on behalf of the Applicant/Subscriber. Delivery of Subscriber's Public Key to HKPost is required together with the Certificate Signing Request (CSR) for generation of Certificate.

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

6.1.4 Key Sizes
The HKPost signing key pair is 2048-bit RSA. Subscriber key pairs for e-Cert (Organisational Role) certificates are 2048-bit RSA.

6.1.5 Standards for Cryptographic Module
Signing key generation, storage, and signing operations performed by HKPost are conducted within a hardware cryptographic module.

6.1.6 Key Usage Purposes
Keys used in e-Cert (Organisational Role) certificates are only used for Digital Signatures and conducting enciphered electronic communications in the Designated Applications for the corresponding e-Cert (Organisational Role) as specified in **Appendix H**. HKPost Root Key (the key used to create or issue certificates that conform to this CPS) is used only for signing (a) certificates and (b) Certificate Revocation Lists.

6.2 Private Key Protection

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

6.2.2 Private Key Multi-Person Control
HKPost Private Keys are stored in tamper-proof hardware cryptographic devices. HKPost implements multi-person control 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 used by HKPost. For backup of HKPost Private Keys, see Section 6.2.4 below.

6.2.4 Backup of HKPost Private Keys

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

6.3 Other Aspects of Key Pair Management

HKPost CA root keys will be used for no more than the lifespan of the respective signing root key and certificates created by HKPost (see **Appendix G** and also Section 4.7). All HKPost key generation, key destruction, key storage, and certificate revocation list signing operations are performed in a hardware cryptographic module. Archival of HKPost Public Keys is performed as specified in Section 4.6.

6.4 Computer Security Controls

HKPost implements multi-person control over the life cycle of activation data such as PINs and passwords for accessing the CA systems. Security procedures are in place to prevent and detect unauthorised access, modification, or compromise of the CA systems. Such security controls are subject to compliance assessment as specified in Section 2.6.

6.5 Life Cycle Technical Security Controls

HKPost implements controls over the procedures for the procurement and development of software and hardware for HKPost 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.

6.6 Network Security Controls

The HKPost CA systems are protected by firewalls and other access control mechanisms configured to allow only authorised access required for the CA services set forth in this CPS.

6.7 Cryptographic Module Engineering Controls

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

7. CERTIFICATE AND CERTIFICATE REVOCATION LIST PROFILES

7.1 Certificate Profile

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

7.2 Certificate Revocation List Profile

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

8. CPS ADMINISTRATION

All changes to this CPS must be approved and published by HKPost. The CPS changes will be effective upon publication by HKPost in the HKPost CA web site at http://www.eCert.gov.hk or in the HKPost Repository and are binding on all Applicants and Subscribers to whom certificates are issued. HKPost will notify the Commissioner for Digital Policy 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.

Appendix A - Glossary

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

"Accept", in relation to a certificate

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

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

"Applicant" means a natural person or legal entity who has applied for an e-Cert (Organisational Role). Once the e-Cert (Organisational Role) is issued, the Applicant is referred to as the Subscriber.

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

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

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

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

"CA" means Certification Authority.

"Certificate" or "e-Cert (Organisational Role)" means a Record which:-

a) is issued by a Certification Authority for the purpose of supporting a Digital Signature which purports to confirm the identity or other significant characteristics of the person who holds a particular key pair;
b) identifies the Certification Authority issuing it;
c) names or identifies the person to whom it is issued;
d) contains the Public Key of the person to whom it is issued; and
e) is Signed by the Certification Authority issuing it.

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

"Certification Practice Statement" or "CPS" means a statement issued by a Certification

Authority to specify the practices and standards that the Certification Authority employs in issuing certificates.

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

"Certificate Signing Request" or "CSR" means a message containing a Public Key of the Subscriber sent by the Registration Office to HKPost via the corresponding Registration Authority in order to apply for a Certificate.

"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 July 2023 to 30 June 2026, and an extended period up to 30 June 2027 (date inclusive).

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

"COP" means the Code of Practice for Recognized Certification Authorities published by the Commissioner for Digital Policy under Section 33 of the Ordinance.

"CPS" means Certification Practice Statement.

"Designated Application" means, a service or system, if any, set out in **Appendix H** in respect of which e-Cert (Organisational Role) certificates of the corresponding organisation are used for.

"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.

"e-Cert Storage Medium" means a storage medium, such as a recordable CD, for storage of the e-Cert and the Private Key.

"Electronic Record" means a Record generated in digital form by an Information System, which can be

(a) transmitted within an Information System or from one Information System to another; and
(b) stored in an Information System or other medium.

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

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

"Hardware Security Module", or "HSM" means a hardware security device used for storage and management of Certificates and protection of key pairs from being tampered, exported or duplicated.

"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).

"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.

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

"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.

"Registration Authority" means Registration Authority.

"Recognized Certificate" means

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

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

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

"Registration Authority" means an organisation that has been appointed by Certizen Limited, if any as listed in **Appendix E (I)**, as its Subcontractor to perform part of the Contract as detailed in this CPS.

"Registration Office" means an organisation that has been authorised by the Subscriber Organisation, if any as listed in **Appendix E (II)**, to manage key pairs and Certificates stored in a Hardware Security Module in order to perform tasks as detailed in **Appendix E (II)**. Members of the Registration Office must not perform the roles and responsibilities of the Registration Authority referred to in **Appendix E (I)**.

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

"Relying Parties" means a natural person or legal entity that have relied on any class or category of e-Cert (Organisational Role), for authorised use of the Certificates in a transaction within the Designated Application of the Subscriber Organisation.

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

"Role" means the title or the position of the Authorised User given by Subscriber Organisation.

"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.

"Sub CA" means the subordinate Certification Authority certificates which are issued by the Root CAs of HKPost and are 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.

Note *:- "holds", in connection to a Private Key, means to keep in one's custody such that only the person named or identified in a certificate, who is duly authorised by the Subscriber Organisation as an Authorised User, can use that Private Key.

"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 an organisation whose Authorised Representative has signed a Subscriber Agreement and to whom a Hongkong Post e-Cert (Organisational Role) has been issued in accordance with the eligibility criteria set out in this CPS.

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

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

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 (Organisational Role) Format

1. Hongkong Post e-Cert (Organisational Role) Format

1.1 Under root CA "Hongkong Post Root CA 2"

For e-Cert (Organisational Role) issued by Sub CA "Hongkong Post e-Cert CA 2 - 15" using SHA-256 hash algorithm: -

Field Name		Field Content
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 2 - 15, o=Hongkong Post, l=Hong Kong, s=Hong Kong, c=HK
Validity period	**Not before**	[UTC time set by HKPost CA system]
	Not after	[UTC time set by HKPost CA system]
Subject name		cn=[Authorised User's name as it appears in the document to verify the identity of the Authorised User of the Subscriber Organisation] (Note 1) e=[email address] (Note 2) ou=[SRN] (Note 3) ou=[BRN+CI/CR+Others] (Note 4) ou=[Subscriber Organisation Name] (Note 5) ou=[Role+' / ' +Subscriber Organisation branch/dept] (Note 6) o=Hongkong Post e-Cert (Organisational Role) 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 7)		
Authority Key Identifier	**Issuer**	cn=Hongkong Post Root CA 2, o=Hongkong Post, l=Hong Kong, s=Hong Kong, c=HK
	Serial number	[Inherited from Issuer]
Key usage		Non-repudiation, Digital Signature, Key Encipherment **(This field will be set Critical.)**
Certificate policies		PolicyIdentifier = [OID] (Note 8) PolicyQualifierID = CPS Qualifier = [URL of CPS] Policy Identifier = 1.3.6.1.4.1.16030.1.4 (Note 9) Policy Qualifier Id = CPS Qualifier = [URL of CPS]
Subject alternative name	**DNS**	Not used
	rfc822	[email address] (Note 2)
	1st Directory Name CN	[An identifier of Authorised User as given by Subscriber Organisation, if any] (Note 10)
Issuer alternate name		Not used

Field Name		Field Content
Basic constraint	**Subject type**	End Entity
	Path length constraint	None
Extended key usage		SSL Client, Adobe Authentic Documents Trust
CRL distribution points		Distribution Point Name = [URL of CRL Distribution Point] (Note 11)
Netscape extension (Note 7)		
Netscape cert type		Not used
Netscape SSL server name		Not used
Netscape comment		Not used

Note

1. Authorised user name as it appears in the document to verify the identity of the Authorised User of the Subscriber Organisation (see Appendix H) with format, for example, Surname (in capital) + Given name (e.g. CHAN Tai Man David).
2. Email address of the Authorised User provided by Subscriber Organisation (blank if null)
3. SRN: 10-digit Subscriber Reference Number
4. Business Registration Certificate Number (BRN): a string of 16 digits/alphabets [filled with all zeroes if BRN is not available]. Certificate of Incorporation (CI)/ Certificate of Registration (CR): a string of 8 digits/alphabets [filled with leading zeros if CI/CR is shorter than 8 digits/alphabets, or all zeroes if CI/CR is not available]. Others: a string of max. 30 digits/alphabets (blank if null). For HKSAR government departments, BRN and CI/CR are filled with zeroes, department name in abbreviation (e.g. HKPO for Hongkong Post) is placed in Others.
5. For organisations who subscribe to e-Cert (Organisational Role) 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).
6. Role is the title or the position of the Authorised User given by the Subscriber Organisation. The separator characters ' / ' (composed of a slash with a space preceding and after the slash) will be included in this field when the Subscriber Organisation branch/dept is not blank.
7. All standard extensions and Netscape extensions are set as "non-critical" unless otherwise specified.
8. The OID of this CPS is included in this field. Please refer to section 1.1 of this CPS for the OID of this CPS.
9. The OID for supporting Adobe PDF signing is added in this field.
10. This field can be a string of max. 30 digits/alphabets, that is used as an identifier of the Authorised User in the Subscriber Organisation, such as a staff number.
11. URL of CRL Distribution Point is http://crl1.eCert.gov.hk/crl/eCertCA2-15CRL2.crl which is a partitioned CRL issued by the Sub CA "Hongkong Post e-Cert CA 2 - 15". (For certificates issued before 1 July 2019, URL of CRL Distribution Point is http://crl1.hongkongpost.gov.hk/crl/eCertCA2-15CRL2.crl)

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

The Appendix C of this CPS provides the arrangement of updating and publishing the Certificate Revocation Lists (CRLs) issued by the Sub CA "Hongkong Post e-Cert CA 2 - 15", as well as the Authority Revocation List (ARL) issued by the Root CA "Hongkong Post Root CA 2". Additionally, it specifies the format of these CRLs and ARL.

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

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

i. Certificates issued by Sub CA "Hongkong Post e-Cert CA 2 - 15":
http://crl1.eCert.gov.hk/crl/eCertCA2-15CRL2.crl (For certificates issued before 1 July 2019, URL of CRL Distribution Point is http://crl1.hongkongpost.gov.hk/crl/eCertCA2-15CRL2.crl)

b) **Full CRL** that contains Information of all suspended or revoked certificates that are issued by the Sub CA "Hongkong Post e-Cert CA 2 - 15". The full CRL is available for public access at the following location (URL):-

i. Certificates issued by Sub CA "Hongkong Post e-Cert CA 2 - 15"
http://crl1.eCert.gov.hk/crl/eCertCA2-15CRL1.crl; or
ldap://ldap1.eCert.gov.hk (port 389, cn=Hongkong Post e-Cert CA 2 - 15 CRL1, o=Hongkong Post, c=HK)

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

Under normal circumstances, HKPost will publish the latest CRL as soon as possible after the update time. HKPost may need to change the above updating and publishing schedule of the 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 List (ARL) containing information of suspended or revoked Sub CA certificates under this CPS. HKPost shall update and publish the ARL annually before its next update date or when necessary. The latest ARL is available at the following location:

i. Sub CA certificates issued by Root CA "Hongkong Post Root CA 2":
http://crl1.eCert.gov.hk/crl/RootCA2ARL.crl or
ldap://ldap1.eCert.gov.hk (port 389, cn=Hongkong Post Root CA 2, o=Hongkong Post, c=HK)

(I) Format of Partitioned and Full CRL issued by the Sub CA "Hongkong Post e-Cert CA 2 - 15" 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		sha256RSA		This field contains the algorithm identifier for the algorithm used to sign the CRL.
Issuer name		cn=Hongkong Post e-Cert CA 2 - 15, o=Hongkong Post, l=Hong Kong,		This field identifies the entity who has signed and issued the CRL.

Standard Fields	Sub-fields	Field Contents of Partitioned CRL	Field Contents of Full CRL	Remarks
		s=Hong Kong, c=HK		
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 2 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 – 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 ARL issued by the root CA "Hongkong Post Root CA 2" 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		sha256RSA	This field contains the algorithm identifier for the algorithm used to sign the ARL.
Issuer name		cn=Hongkong Post Root CA 2 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.

Standard Fields	Sub-fields	Field Contents of ARL	Remarks
Next update		[UTC time]	"Next Update" contains the date by which the next ARL will be issued, but it will not be issued any later than the indicated date. Notwithstanding this, the ARL is updated and issued on an **annual** basis as stated in the CPS.
Revoked certificates	**User certificate**	[Certificate Serial Number]	Revoked certificates are listed by their serial numbers.
	Revocation date	[UTC time]	The date on which the revocation occurred is specified.
	CRL entry extensions		
	Reason code	[Revocation Reason Code]	(Note 1)
Standard extension (Note 2)			
Authority Key Identifier	**Issuer**	cn=Hongkong Post Root CA2 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.)**	

Note

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

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

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

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

Appendix D - Summary of Hongkong Post e-Cert (Organisational Role) Features

Features[Note 1]	**e-Cert (Organisational Role) Certificate**
Subscriber	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 SAR and bureaux, departments of Government of HKSAR.
Certificate holders	Authorised Users who are members or employees of the Organisation as the Subscriber
Reliance Limit	HK$15,000
Recognized Certificate	Yes
Key pair size	2048-bit RSA
Registration Authority	See **Appendix E**
Key pair generation	By Hongkong Post on behalf of the Subscriber through the central key generation service
Identity verification	Authentication of the identity of the organization and its Authorised Representative
Usage of certificate	Digital Signature and Encryption in the Designated Applications of the corresponding e-Cert (Organisational Role) as specified in **Appendix H**
Subscriber's information included in the certificate	▪ Subscriber Organisation's name ▪ Authorised User's name and email address; ▪ Authorised User's Role in the Subscriber Organisation ▪ Subscriber Reference Number (SRN) generated by the HKPost system ▪ Subscriber Organisation's company/business registration information ▪ An identifier of Authorised User as given by the Subscriber Organisation
Subscription fees and certificate validity	Certificate validity is one year. See **Appendix H**

Note

1. Prior arrangement between the subscriber and HKPost is required before HKPost will issue e-Cert (Organisational Role) certificates for that subscriber.

Appendix E - List of Registration Authorities and Registration Office for the Hongkong Post e-Cert (Organisational Role), if any

(I) List of Registration Authorities

Name of Registration Authorities	Classes of Certificate(s)	Address of Service Outlets & Business Hours	Services to be Provided	Remarks
Corporate Information Security and Privacy Office, Hospital Authority / www.ha.org.hk	Hongkong Post e-Cert (Organisational Role) for Hospital Authority	Hospital Authority Building, 147B Argyle Street, Kowloon, Hong Kong 9:00 am to 5:00 pm daily, except Saturdays, Sundays and public holidays	The following processes of e-Cert (Organisational Role) applications for Hospital Authority:- - certificate applications as set out in Sections 3.1.8 and 4.1. - certificate renewal request as set out in Section 3.2. - certificate revocation and suspension request as set out in Section 4.4.1, 4.4.2 and 4.4.3. - protection of paper documents as set out in Section 5.1.8, and execute procedures as required by HKPost for compliance to Sections 4.5, 4.6 and 5.1.	It is a sub-contractor of the Contractor (and therefore also acting for HKPost) in performing functions including verification of the identity of the Applicant and also the identity and due authorisation of the Authorised Representative(s) and Authorised User(s) of the Applicant, at the time of application of an e-Cert (Organisational Role) by the Applicant (first time or renewal). Similarly, verification of the identity of the Subscriber (and of its Authorised Representative or Authorised User) in the case of any revocation request from such Subscriber.
Information Technology section, CUHK Medical Centre / www.cuhkmc.hk	Hongkong Post e-Cert (Organisational Role) for CUHK Medical Centre	9 Chak Cheung Street, Shatin, Hong Kong 9:00 am to 5:00 pm daily, except Saturdays, Sundays and public holidays	The following processes of e-Cert (Organisational Role) applications for CUHK Medical Centre:- - certificate applications as set out in Sections 3.1.8 and 4.1.	It is a sub-contractor of the Contractor (and therefore also acting for HKPost) in performing functions including verification of the identity of the Applicant and also the identity and due

Name of Registration Authorities	Classes of Certificate(s)	Address of Service Outlets & Business Hours	Services to be Provided	Remarks
			- certificate renewal request as set out in Section 3.2. - certificate revocation and suspension request as set out in Section 4.4.1, 4.4.2 and 4.4.3. - protection of paper documents as set out in Section 5.1.8, and execute procedures as required by HKPost for compliance to Sections 4.5, 4.6 and 5.1.	authorisation of the Authorised Representative(s) and Authorised User(s) of the Applicant, at the time of application of an e-Cert (Organisational Role) by the Applicant (first time or renewal). Similarly, verification of the identity of the Subscriber (and of its Authorised Representative or Authorised User) in the case of any revocation request from such Subscriber.
Information Technology section, Gleneagles Hospital / www.gleneagles.hk	Hongkong Post e-Cert (Organisational Role) for Gleneagles Hospital	1 Nam Fung Path, Wong Chuk Hang, Hong Kong 9:00 am to 5:00 pm daily, except Saturdays, Sundays and public holidays	The following processes of e-Cert (Organisational Role) applications for Gleneagles Hospital:- - certificate applications as set out in Sections 3.1.8 and 4.1. - certificate renewal request as set out in Section 3.2. - certificate revocation and suspension request as set out in Section 4.4.1, 4.4.2 and 4.4.3. - protection of paper documents as set out in Section 5.1.8, and execute procedures as required by HKPost for compliance to Sections 4.5, 4.6 and 5.1.	It is a sub-contractor of the Contractor (and therefore also acting for HKPost) in performing functions including verification of the identity of the Applicant and also the identity and due authorisation of the Authorised Representative(s) and Authorised User(s) of the Applicant, at the time of application of an e-Cert (Organisational Role) by the Applicant (first time or renewal). Similarly, verification of the identity of the Subscriber (and of its Authorised Representative or Authorised User) in the case of any revocation request from such Subscriber.

Name of Registration Authorities	Classes of Certificate(s)	Address of Service Outlets & Business Hours	Services to be Provided	Remarks
Information Technology section, Chinese Medicine Hospital of Hong Kong / www.cmhhk.org.hk	Hongkong Post e-Cert (Organisational Role) for Chinese Medicine Hospital of Hong Kong	1 Pak Shing Kok Road in Tseung Kwan O, Hong Kong 9:00 am to 5:00 pm daily, except Saturdays, Sundays and public holidays	The following processes of e-Cert (Organisational Role) applications for Chinese Medicine Hospital of Hong Kong:- - certificate applications as set out in Sections 3.1.8 and 4.1. - certificate renewal request as set out in Section 3.2. - certificate revocation and suspension request as set out in Section 4.4.1, 4.4.2 and 4.4.3. - protection of paper documents as set out in Section 5.1.8, and execute procedures as required by HKPost for compliance to Sections 4.5, 4.6 and 5.1.	It is a sub-contractor of the Contractor (and therefore also acting for HKPost) in performing functions including verification of the identity of the Applicant and also the identity and due authorisation of the Authorised Representative(s) and Authorised User(s) of the Applicant, at the time of application of an e-Cert (Organisational Role) by the Applicant (first time or renewal). Similarly, verification of the identity of the Subscriber (and of its Authorised Representative or Authorised User) in the case of any revocation request from such Subscriber.

(II) List of Registration Offices

Name of Registration Offices	Classes of Certificate(s)	Address of Service Outlets & Business Hours	Services to be Provided	Remarks
Clinical System Development Section, Hospital Authority	Hongkong Post e-Cert (Organisational Role) for Hospital Authority	Hospital Authority Building, 147B Argyle Street, Kowloon, Hong Kong 9:00 am to 5:00 pm daily, except Saturdays, Sundays and public holidays	The following processes of e-Cert (Organisational Role) applications for Hospital Authority:- - key generation as set out in Sections 3.1.7, 3.2 and 4.2. - take responsibilities of the obligations as set out in Section 2.1.4.	Registration Office must appoint the Authorised Representative ("AR") who apply for e-Cert (Organisational Role). Neither AR nor Registration Office are the persons or members of the Registration Authority ("Registration Authority") nominated to perform the roles and responsibilities of the Registration Authority referred to in **Appendix E (I)**.
Human Resource section, CUHK Medical Centre	Hongkong Post e-Cert (Organisational Role) for CUHK Medical Centre	9 Chak Cheung Street, Shatin, Hong Kong 9:00 am to 5:00 pm daily, except Saturdays, Sundays and public holidays	The following processes of e-Cert (Organisational Role) applications for CUHK Medical Centre:- - key generation as set out in Sections 3.1.7, 3.2 and 4.2. - take responsibilities of the obligations as set out in Section 2.1.4.	Registration Office must appoint the Authorised Representative ("AR") who apply for e-Cert (Organisational Role). Neither AR nor Registration Office are the persons or members of the Registration Authority ("Registration Authority") nominated to perform the roles and responsibilities of the Registration Authority referred to in **Appendix E (I)**.

Name of Registration Offices	Classes of Certificate(s)	Address of Service Outlets & Business Hours	Services to be Provided	Remarks
Human Resource section, Gleneagles Hospital	Hongkong Post e-Cert (Organisational Role) for Gleneagles Hospital	1 Nam Fung Path, Wong Chuk Hang, Hong Kong 9:00 am to 5:00 pm daily, except Saturdays, Sundays and public holidays	The following processes of e-Cert (Organisational Role) applications for Gleneagles Hospital:- - key generation as set out in Sections 3.1.7, 3.2 and 4.2. - take responsibilities of the obligations as set out in Section 2.1.4.	Registration Office must appoint the Authorised Representative ("AR") who apply for e-Cert (Organisational Role). Neither AR nor Registration Office are the persons or members of the Registration Authority ("Registration Authority") nominated to perform the roles and responsibilities of the Registration Authority referred to in **Appendix E (I)**.
Human Resource section, Chinese Medicine Hospital of Hong Kong	Hongkong Post e-Cert (Organisational Role) for Chinese Medicine Hospital of Hong Kong	1 Pak Shing Kok Road in Tseung Kwan O, Hong Kong 9:00 am to 5:00 pm daily, except Saturdays, Sundays and public holidays	The following processes of e-Cert (Organisational Role) applications for Chinese Medicine Hospital of Hong Kong:- - key generation as set out in Sections 3.1.7, 3.2 and 4.2. - take responsibilities of the obligations as set out in Section 2.1.4.	Registration Office must appoint the Authorised Representative ("AR") who apply for e-Cert (Organisational Role). Neither AR nor Registration Office are the persons or members of the Registration Authority ("Registration Authority") nominated to perform the roles and responsibilities of the Registration Authority referred to in **Appendix E (I)**.

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

Name of Subcontractor / web site	Classes of Certificate(s)	Services to be Provided
Hospital Authority / www.ha.org.hk	e-Cert (Organisational Role) certificates for Hospital Authority	Referred to **Appendix E** for the services to be provided.
CUHK Medical Centre / www.cuhkmc.hk	e-Cert (Organisational Role) certificates for CUHK Medical Centre	Referred to **Appendix E** for the services to be provided.
Gleneagles Hospital / www.gleneagles.hk	e-Cert (Organisational Role) certificates for Gleneagles Hospital	Referred to **Appendix E** for the services to be provided.
Chinese Medicine Hospital of Hong Kong / www.cmhhk.org.hk	e-Cert (Organisational Role) certificates for Chinese Medicine Hospital of Hong Kong	Referred to **Appendix E** for the services to be provided.

Appendix G - Lifespan of CA root certificates

Name of the root certificate	Lifespan	Remarks
Hongkong Post Root CA 2	5 September 2015 – 5 September 2040	
Hongkong Post e-Cert CA 2 - 15	7 July 2026 – 5 September 2030	This Sub CA is reissued without rekey by the Root CA "Hongkong Post Root CA 2" to issue e-Cert (Organisational Role) to applicants with effect from 1 October 2026.

Appendix H - List of Subscriber Organisations and the corresponding Designated Applications of Hongkong Post e-Cert (Organisational Role) Certificates

Name of Subscriber Organisation	Corresponding Registration Authority, if any	Documents to verify the identity of Authorised User of the Subscriber Organisation(Note 1)	Certificate Validity (Note 2)	Designated Application	Subscription Fees
Hospital Authority	Hospital Authority	Computer record in the Human Capital Management System of Hospital Authority	1 year	Applicable to the Hospital Authority's internal systems only.	New application or renewal : HK$150 per certificate; and an administration fee (irrespective of the number of Authorised Users) : HK$150 per application.
CUHK Medical Centre	CUHK Medical Centre	Computer record in the Human Capital Management System of CUHK Medical Centre	1 year	Applicable to the CUHK Medical Centre's internal systems only for digital signing of medical prescriptions.	New application or renewal : HK$150 per certificate; and an administration fee (irrespective of the number of Authorised Users) : HK$150 per application.
Gleneagles Hospital	Gleneagles Hospital	Computer record in the Human Capital Management System of Gleneagles Hospital	1 year	Applicable to the Gleneagles Hospital's internal systems only for digital signing of medical order requests and/or medical certificates.	New application or renewal : HK$150 per certificate; and an administration fee (irrespective of the number of Authorised Users) : HK$150 per application.

Name of Subscriber Organisation	Corresponding Registration Authority, if any	Documents to verify the identity of Authorised User of the Subscriber Organisation(Note 1)	Certificate Validity (Note 2)	Designated Application	Subscription Fees
Chinese Medicine Hospital of Hong Kong	Chinese Medicine Hospital of Hong Kong	Computer record in the Human Capital Management System of Chinese Medicine Hospital of Hong Kong	1 year	Applicable to the internal systems of Chinese Medicine Hospital of Hong Kong only for digital signing of medical order requests and/or medical certificates.	New application or renewal : HK$150 per certificate; and an administration fee (irrespective of the number of Authorised Users) : HK$150 per application.

Note

1. The documents shall contain the documentary evidence, e.g. HKID Card or passport information, as to be usable for subsequent reference to verify the identity of the Authorised User.
2. See also section 3.2.2 of this CPS.