THE CERTIFICATION PRACTICE STATEMENT

OF

THE POSTMASTER GENERAL

As

A Recognized Certification Authority
under the Electronic Transactions Ordinance

for

Hongkong Post g-Cert (Individual)
Hongkong Post g-Cert (Functional Unit)
with S/MIME Functions

Date : 25 November 2026
OID : 1.3.6.1.4.1.16030.1.8.16

Table of Contents

PREAMBLE 8
1. INTRODUCTION 10
1.1 Overview 10
1.2 Document Name and Identification 10
1.3 PKI Participants 11
1.3.1 Certification Authorities 11
1.3.2 Registration Authorities 12
1.3.3 Centrally Managed Messaging Platform 12
1.3.4 Subscribers 13
1.3.5 Relying Parties 14
1.3.6 Other participants 14
1.4 Certificate Usage 15
1.4.1 Appropriate Certificate Uses 15
1.4.2 Prohibited Certificate Uses 15
1.5 Policy Administration 15
1.5.1 Organisation Administering the Document 15
1.5.2 Contact Person 15
1.5.3 Person Determining CPS Suitability for the Policy 15
1.5.4 CPS Approval Procedures 16
1.6 Definitions and Acronyms 16
2. Publication and Repository Responsibilities 17
2.1 Repositories 17
2.2 Publication of Certification Information 17
2.3 Time or Frequency of Publication 17
2.4 Access Controls on Repositories 17
3. Identification and Authentication 18
3.1 Naming 18
3.1.1 Types of Names 18
3.1.2 Need for Names to be Meaningful 18
3.1.3 Anonymity or Pseudonymity of Subscribers 18
3.1.4 Rules for Interpreting Names 18
3.1.5 Uniqueness of Names 19
3.1.6 Recognition, Authentication, and Role of Trademarks 19
3.2 Initial Identity Validation 19
3.2.1 Method to Prove Possession of Private Key 19
3.2.2 Authentication of Organisation Identity 20
3.2.3 Authentication of Individual Identity 20
3.2.4 Non-Verified Subscriber Information 20
3.2.5 Validation of Authority and Mailbox Control 20
3.2.6 Criteria for Interoperation 20
3.3 Identification and Authentication for Re-Key Requests 21
3.3.1 Identification and Authentication for Routine Re-Key 21
3.3.2 Identification and Authentication for Re-Key After Revocation 21
3.4 Identification and Authentication for Revocation Requests 21
4. Certificate Life-Cycle Operational Requirements 22
4.1 Certificate Application 22
4.1.1 Who Can Submit a Certificate Application 22
4.1.2 Enrolment Process and Responsibilities 22
4.2 Certificate Application Processing 22

4.2.1 Performing Identification and Authentication Functions....22
4.2.2 Approval or Rejection of Certificate Applications....23
4.2.3 Time to Process Certificate Applications....23
4.3 Certificate Issuance....23
4.4 Certificate Acceptance....23
4.4.1 Conduct Constituting Certificate Acceptance....23
4.4.2 Publication of the Certificate by the CA....23
4.4.3 Notification of Certificate Issuance by the CA to Other Entities....23
4.5 Key Pair and Certificate Usage....23
4.5.1 Subscriber Private Key and Certificate Usage....24
4.5.2 Relying Party Public Key and Certificate Usage....24
4.6 Certificate Renewal....24
4.6.1 Circumstances for Renewal....24
4.6.2 Who May Request Renewal....24
4.6.3 Processing Renewal Requests....25
4.6.4 Notification of New Certificate Issuance to Subscriber....25
4.6.5 Conduct Constituting Acceptance of a Renewal Certificate....25
4.6.6 Publication of the Renewal Certificate by the CA....25
4.6.7 Notification of Certificate Issuance by the CA to Other Entities....25
4.7 Certificate Re-Key....25
4.7.1 Circumstances for Certificate Re-Key....25
4.7.2 Who May Request Certification of a New Public Key....26
4.7.3 Processing Certificate Re-Keying Requests....26
4.7.4 Notification of New Certificate Issuance to Subscriber....26
4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate....26
4.7.6 Publication of the Re-Keyed Certificate by the CA....26
4.7.7 Notification of Certificate Issuance by the CA to Other Entities....26
4.8 Certificate Modification....26
4.8.1 Circumstances for Certificate Modification....26
4.8.2 Who May Request Certificate Modification....26
4.8.3 Processing Certificate Modification Requests....26
4.8.4 Notification of New Certificate Issuance to Subscriber....26
4.8.5 Conduct Constituting Acceptance of Modified Certificate....26
4.8.6 Publication of the Modified Certificate by the CA....26
4.8.7 Notification of Certificate Issuance by the CA to Other Entities....27
4.9 Certificate Revocation and Suspension....27
4.9.1 Circumstances for Revocation....27
4.9.2 Who Can Request Revocation....28
4.9.3 Procedure for Revocation Request....29
4.9.4 Revocation Request Grace Period....29
4.9.5 Time within Which CA Must Process the Revocation Request....30
4.9.6 Revocation Checking Requirements for Relying Parties....30
4.9.7 CRL Issuance Frequency....30
4.9.8 Maximum Latency for CRLs....30
4.9.9 On-Line Revocation/Status Checking Availability....30
4.9.10 On-Line Revocation Checking Requirements....31
4.9.11 Other Forms of Revocation Advertisements Available....31
4.9.12 Special Requirements Related to Key Compromise....31
4.9.13 Circumstances for Suspension....31
4.9.14 Who Can Request Suspension....31

4.9.15 Procedure for Suspension Request....31
4.9.16 Limits on Suspension Period....31
4.10 Certificate Status Services....31
4.10.1 Operational Characteristics....31
4.10.2 Service Availability....31
4.10.3 Operational Features....31
4.11 End of Subscription....31
4.12 Key Escrow and Recovery....32
4.12.1 Key Escrow and Recovery Policy and Practices....32
4.12.2 Session Key Encapsulation and Recovery Policy and Practices....32
5. Facility, Management, and Operational Controls....33
5.1 Physical Controls....33
5.1.1 Site Location and Construction....33
5.1.2 Physical Access....33
5.1.3 Power and Air Conditioning....33
5.1.4 Water Exposures....33
5.1.5 Fire Prevention and Protection....33
5.1.6 Media Storage....33
5.1.7 Waste Disposal....34
5.1.8 Off-site Backup....34
5.2 Procedural Controls....34
5.2.1 Trusted Roles....34
5.2.2 Number of Personnel Needed for Each Task....34
5.2.3 Identification and Authentication of Each Role....34
5.2.4 Roles requiring Segregation of Duties....34
5.3 Personnel Controls....34
5.3.1 Qualifications, Experience, and Clearance Requirements....35
5.3.2 Background Check Procedures....35
5.3.3 Training Requirements....35
5.3.4 Retraining Frequency and Requirements....35
5.3.5 Job Rotation Frequency and Sequence....35
5.3.6 Sanctions for Unauthorised Actions....35
5.3.7 Independent Contractor Requirements....36
5.3.8 Documentation Supplied to Personnel....36
5.4 Audit Logging Procedures....36
5.4.1 Types of Events Recorded....36
5.4.2 Frequency of Processing Log....37
5.4.3 Retention Period for Audit Log....37
5.4.4 Protection of Audit Log....37
5.4.5 Audit Log Backup Procedures....37
5.4.6 Audit Collection System (Internal vs. External)....37
5.4.7 Notification to Event-Causing Subject....37
5.4.8 Vulnerability Assessments....37
5.5 Records Archival....37
5.5.1 Types of Records Archived....37
5.5.2 Retention Period for Archive....38
5.5.3 Protection of Archive....38
5.5.4 Archive Backup Procedures....38
5.5.5 Requirements for Time-Stamping of Records....38
5.5.6 Archive Collection System (Internal or External).....38

5.5.7 Procedures to Obtain and Verify Archive Information 38
5.6 Key Changeover 38
5.7 Compromise and Disaster Recovery 38
5.7.1 Incident and Compromise Handling Procedures 38
5.7.2 Computing Resources, Software, and/or Data Are Corrupted 39
5.7.3 Entity Private Key Compromise Procedures 39
5.7.4 Business Continuity Capabilities after a Disaster 39
5.8 CA or RA Termination 40
6. Technical Security Controls 41
6.1 Key Pair Generation and Installation 41
6.1.1 Key Pair Generation 41
6.1.2 Private Key Delivery to Subscriber 41
6.1.3 Public Key Delivery to Certificate Issuer 41
6.1.4 CA Public Key Delivery to Relying Parties 41
6.1.5 Key Sizes 41
6.1.6 Public Key Parameters Generation and Quality Checking 41
6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field) 41
6.2 Private Key Protection and Cryptographic Module Engineering Controls 42
6.2.1 Cryptographic Module Standards and Controls 42
6.2.2 Private Key (n out of m) Multi-Person Control 42
6.2.3 Private Key Escrow 42
6.2.4 Private Key Backup 42
6.2.5 Private Key Archival 42
6.2.6 Private Key Transfer between Cryptographic Modules 42
6.2.7 Private Key Storage on Cryptographic Module 42
6.2.8 Method of Activating Private Key 42
6.2.9 Method of Deactivating Private Key 42
6.2.10 Method of Destroying Private Key 43
6.2.11 Cryptographic Module Rating 43
6.3 Other Aspects of Key Pair Management 43
6.3.1 Public Key Archival 43
6.3.2 Certificate Operational Periods and Key Pair Usage Periods 43
6.4 Activation Data 43
6.4.1 Activation Data Generation and Installation 43
6.4.2 Activation Data Protection 43
6.4.3 Other Aspects of Activation Data 44
6.5 Computer Security Controls 44
6.5.1 Specific Computer Security Technical Requirements 44
6.5.2 Computer Security Rating 44
6.6 Life Cycle Technical Controls 44
6.6.1 System Development Controls 44
6.6.2 Security Management Controls 44
6.6.3 Life Cycle Security Controls 45
6.7 Network Security Controls 45
6.8 Time-Stamping 45
7. Certificate, CRL, and OCSP Profiles 46
7.1 Certificate Profile 46
7.1.1 Version Number(s) 46
7.1.2 Certificate Extensions 46
7.1.3 Algorithm Object Identifiers 46

7.1.4 Name Forms 46
7.1.5 Name Constraints 46
7.1.6 Certificate Policy Object Identifier 46
7.1.7 Usage of Policy Constraints Extension 46
7.1.8 Policy Qualifiers Syntax and Semantics 46
7.1.9 Processing Semantics for the Critical Certificate Policies Extension 46
7.2 CRL Profile 46
7.2.1 Version Number(s) 50
7.2.2 CRL and CRL Entry Extensions 50
7.3 OCSP Profile 50
7.3.1 Version Number(s) 50
7.3.2 OCSP Extensions 50
8. Compliance Audit and Other Assessments 51
8.1 Frequency and Circumstances of Assessment 51
8.2 Identity/Qualifications of Assessor 51
8.3 Assessor's Relationship to Assessed Entity 51
8.4 Topics Covered by Assessment 51
8.5 Actions Taken as a Result of Deficiency 51
8.6 Communications of Results 51
8.7 Self-Audits 51
9. Other Business and Legal Matters 52
9.1 Fees 52
9.1.1 Certificate Issuance or Renewal Fees 52
9.1.2 Certificate Access Fees 52
9.1.3 Revocation or Status Information Access Fees 52
9.1.4 Fees for Other Services 52
9.1.5 Refund Policy 52
9.2 Financial Responsibility 52
9.2.1 Insurance Coverage 52
9.2.2 Other Assets 52
9.2.3 Insurance or Warranty Coverage for End-Entities 52
9.3 Confidentiality of Business Information 53
9.3.1 Scope of Confidential Information 53
9.3.2 Information Not Within the Scope of Confidential Information 53
9.3.3 Responsibility to Protect Confidential Information 53
9.4 Privacy of Personal Information 53
9.4.1 Privacy Plan 53
9.4.2 Information Treated as Private 53
9.4.3 Information Not Deemed Private 53
9.4.4 Responsibility to Protect Private Information 53
9.4.5 Notice and Consent to Use Private Information 54
9.4.6 Disclosure Pursuant to Judicial or Administrative Process 54
9.4.7 Other Information Disclosure Circumstances 54
9.5 Intellectual Property Rights 54
9.6 Representations and Warranties 54
9.6.1 CA Representations and Warranties 54
9.6.2 RA Representations and Warranties 55
9.6.3 Subscriber Representations and Warranties 55
9.6.4 Relying Party Representations and Warranties 56
9.6.5 Representations and Warranties of Other Participants 56

9.7 Disclaimers of Warranties 58
9.8 Limitations of Liability 59
9.9 Indemnities 60
9.10 Term and Termination 62
9.10.1 Term 62
9.10.2 Termination 62
9.10.3 Effect of Termination and Survival 62
9.11 Individual Notices and Communications with Participants 63
9.12 Amendments 63
9.12.1 Procedure for Amendment 63
9.12.2 Notification Mechanism and Period 63
9.12.3 Circumstances Under Which OID Must be Changed 63
9.13 Dispute Resolution Provisions 63
9.14 Governing Law 64
9.15 Compliance with applicable law 64
9.15.1 Jurisdiction 64
9.16 Miscellaneous Provisions 64
9.16.1 Entire Agreement 64
9.16.2 Assignment 64
9.16.3 Severability 64
9.16.4 Enforcement (Non-Waiver of Rights) 64
9.16.5 Force Majeure 64
9.17 Other Provisions 65
9.17.1 No Supply of Goods 65
Appendix A - Glossary and Acronyms 66
Appendix B - Hongkong Post g-Cert Format 72
Appendix C - Hongkong Post Certificate Revocation Lists (CRLs) and Authority Revocation List (ARL) Format 75
Appendix D - Summary of Hongkong Post g-Cert Features 78
Appendix E - List of Subscriber Organisation / Registration Authorities and CMMP for the Hongkong Post g-Cert, if any 79
Appendix F - List of Subcontractor(s) of Certizen Limited for Hongkong Post g-Cert Services, if any 85
Appendix G - Lifespan of CA root certificates 86
Appendix H - List of the Designated Applications of Hongkong Post g-Cert Certificates 87

© 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. A message that is protected using a Public Key can only be decrypted using its corresponding Private Key, and a message that is digitally signed using a Private Key can only be verified using its corresponding Public Key.

The PKI is designed to support secure electronic transactions and communications in the Hong Kong Special Administrative Region (**"Hong Kong SAR"**), including secure electronic mail communications using Secure/Multipurpose Internet Mail Extensions (**S/MIME**).

Under the Ordinance, the Postmaster General is a Recognized Certification Authority (**"CA"**). The Postmaster General performs the functions and provides the services of a CA through the officers of the Hong Kong Post Office and is referred to in this Certification Practice Statement ("CPS") as Hongkong Post or HKPost.

Since 1 April 2007, the operations of the HKPost CA have been outsourced with private sector participation. HKPost has awarded a contract (**"Contract"**) to Certizen Limited for operating and maintaining the systems and services of the HKPost CA for the period from 1 July 2023 to 30 June 2026, and an extended period up to 30 June 2027 (date inclusive). So references to all acts to be performed by HKPost shall include all such acts to be performed by Certizen Limited on behalf of HKPost.

Under the Contract, Certizen Limited may, after obtaining the prior written consent of HKPost, appoint subcontractor(s) for the performance of part of the Contract. A list of such subcontractor(s), if any, is set out in **Appendix F**. Certizen Limited, together with its subcontractor(s), if any, is hereafter referred to as the **"Contractor"** for the purposes of this CPS.

HKPost remains a Recognized CA under Section 34 of the Ordinance, and the Contractor acts as 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, and publication in a publicly available Repository of recognized and accepted digital certificates for secure on-line identification. **The secure electronic mail certificates issued under this CPS (i.e. g-Cert) are Recognized Certificates under the Ordinance and are referred to as "certificates" or "g-Certs" in this CPS.**

This CPS sets out the practices and standards applicable to g-Cert issued by HKPost. Certificates governed by this CPS are issued solely for secure electronic mail (S/MIME) purposes and are issued in compliance with the CA/Browser Forum Baseline Requirements for S/MIME.

Under the Ordinance, HKPost may do anything expedient for the performance of the functions and provision of the services of a CA. In accordance with the Code of Practice for Recognized Certification Authorities, HKPost may appoint agents or subcontractors to carry out some or all of its operations.

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

Save in the case of any negligence or fraud or acting outside the permitted scope of authority or other similar circumstances, HKPost is responsible for the conduct and activities of the RAs in carrying out the functions or providing the services of HKPost as its agents as a Recognized CA in respect of the issuing and revocation of g-Certs.

This CPS sets out practices and standards for g-Certs.

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

This CPS is designed to meet, and HKPost shall operate in accordance with, the latest version of the requirements of the following schemes:

- the Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates ("S/MIME BR") published by the CA / Browser Forum;
- WebTrust Principles and Criteria for Certification Authorities;
- WebTrust Principles and Criteria for Certification Authorities – S/MIME

HKPost will review this CPS periodically and update it as necessary to ensure it remains an accurate description of HKPost's practices and consistent with the latest applicable requirements.

1. INTRODUCTION

1.1 Overview

This Certification Practice Statement ("CPS"), being a combined Certificate Policy ("CP") and Certification Practice Statement document, is published for public knowledge by HKPost and specifies the practices and standards that HKPost employs in issuing, revoking and publishing g-Cert.

HKPost shall maintain this CPS in compliance with the Electronic Transactions Ordinance (Cap. 553) and relevant regulations of the Code of Practice for Recognized Certification Authorities ("Code of Practice") of Hong Kong.

Furthermore, HKPost explicitly adheres to the latest published versions of the Common CA Database (CCADB) Policy. In the event of any conflict between this CPS and the CCADB Policy, the CCADB Policy shall take precedence.

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 g-Cert issued under this CPS and describes the operational, procedural, and security requirements of HKPost.

Certificates issued by HKPost in accordance with this CPS will be relied upon by Relying Parties and used to verify digital signatures and secure electronic mail communications. Each Relying Party making use of a HKPost issued certificate must make an independent determination that PKI based digital signatures and secure electronic mail are appropriate and sufficiently trusted for its particular application.

Under the Ordinance HKPost is a Recognized CA. HKPost has designated the g-Cert (Individual) and g-Cert (Functional Unit) issued under this CPS as Recognized Certificates. This means for both Subscribers and Relying Parties that HKPost has a legal obligation under the Ordinance to use a Trustworthy System for the issuance, revocation, and publication in a publicly available Repository of accepted Recognized Certificates.

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

In this CPS, references to the "S/MIME BR" mean the latest version of those requirements that is effective and applicable to the Recognized Certificates described in this CPS. Where this CPS refers to a specific section, sub-section, appendix, or version of the S/MIME BR, that reference shall be read as including any successor, renumbered, amended, restated, or replacement provision in the latest S/MIME BR. In the event of any inconsistency between this CPS and the latest applicable S/MIME BR, HKPost will comply with the latest applicable S/MIME BR and will update this CPS as soon as reasonably practicable.

A summary of the features of the g-Cert issued under this CPS is set out in **Appendix D**.

1.2 Document Name and Identification

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

Version Number	Revision Description	Effective Date
1 (.14)	First version to replace the existing Certification Practice Statement (OID 1.3.6.1.4.1.16030.1.8.13) for issuing g-Cert (Individual/Functional Unit) in alignment with RFC 3647.	1 October 2026
2 (.15)	Adjust the maximum validity period of g-Cert from 2 years to 1 year for enhancing security and reliability.	1 November 2026
3 (.16)	- Update Section 1.1 to explicitly state that HKPost's adherence to the latest published version of the CCADB Policy. - Update Appendix B to state all standard extensions are set as "non-critical" unless otherwise specified. - Refine wording to align CPS with latest applicable S/MIME BR and fix some typos. - Remove revocation reason code "0" from CRL and ARL. - Align the format of revocation reason codes for CRL and ARL.	25 November 2026

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**") "**1.3.6.1.4.1.16030.1.8.16**" (see description of the field "Certificate Policies" in **Appendix B**). In addition to this OID, all certificates that comply with the Baseline Requirements for S/MIME will include the following additional identifiers:-

g-Cert	Policy Object Identifier (OID)
g-Cert (Individual) certificates	2.23.140.1.5.3.3 (assigned by the CA / Browser Forum, for certificates complying with Sponsor -validated Strict Certificate Policy)
g-Cert (Functional Unit) certificates	2.23.140.1.5.2.3 (assigned by the CA / Browser Forum, for certificates complying with Organisation-validated Strict Certificate Policy)

1.3 PKI Participants

1.3.1 Certification Authorities

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

HKPost's obligations to Subscribers are defined and limited by this CPS and by the terms of the contracts with Subscribers in the form of a Subscriber Agreement. This is so whether the Subscriber is also a Relying Party in relation to a certificate of another Subscriber. In relation to Relying Parties who are not Subscribers, this CPS gives them notice that HKPost undertakes

only to exercise reasonable care and skill to avoid causing certain categories of loss and damage to Relying Parties in issuing, revoking and publishing certificates in conformity with the Ordinance and this CPS, and places a monetary limit in respect of such liability as it may have as set out below and in the certificates issued.

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

a) issue and publish certificates in a timely manner (see Section 2.3);
b) notify Applicants of the approval or rejection of their applications (see Sections 4.1 to 4.4);
c) revoke certificates and publish Certificate Revocation Lists in a timely manner (see Section 4.9); and
d) notify Subscribers of the revocation of their certificates (see Section 4.9.5).

1.3.2 Registration Authorities

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

RAs carry out on HKPost's behalf HKPost's obligations and duties in these matters. RAs have the authority to act on behalf of HKPost to enforce the terms of the Subscriber Agreements (unless and until that authority is withdrawn and Subscribers duly notified of any such withdrawal).

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

1.3.3 Centrally Managed Messaging Platform

Centrally Managed Messaging Platform under the administration and support of DPO (hereafter referred to as CMMP) is to provide various Designated Applications in **Appendix H** for use by Bureau/Department/Office of the Government of Hong Kong SAR ("B/D/O"). The CMMP will adopt X.509 v3 digital certificates, the new special purpose digital certificates issued by Hongkong Post Certification Authority (HKPCA), to handle restricted information

HKPost deals with the Applicant or Subscriber of g-Cert via the role of Requester assigned in CMMP. In this regard, CMMP is the agent serving the Applicant for and Subscriber of g-Cert.

At the same time, the role of Business Administrator is assigned by B/D/O in CMMP to verify the identity of the CMMP user or functional unit for g-Cert. In this regard, Business Administrator acts as Registration Authority for g-Cert (hereafter referred to as Registration Authority ("RA")).

All other functions and obligations, including the functions to be performed by CMMP arising from the certificate life-cycle management and the usage from time to time of the g-Cert, regardless of the nature of the Designated Application, are functions and obligations undertaken

by CMMP whether as principal or as agent for its Subscriber but not as sub-contractor or agent for the Contractor and for HKPost.

1.3.4 Subscribers

Under this CPS, a Subscriber are those B/D/Os listed in Appendix E. They may be referred to as "Applicant" or "Subscriber" or Subscriber Organisation" or "B/D/O". The actual users of g-Certs and affiliated with the Subscriber as the two classes as further described below.

1.3.4.1 Classes of users affiliated with the Subscriber

1.3.4.1.1 g-Cert (Individual) Certificates

A g-Cert (Individual) is issued to CMMP Users at the request of the Requester acting on behalf of B/D/Os (viz the Applicant and the "Subscriber Organisation" as listed in Appendix E); and the g-Cert identifies the CMMP User of a Subscriber Organisation whom that Subscriber Organisation has duly authorised the use of Private Key of that g-Cert (Individual) issued to that Subscriber Organisation. Offer of g-Cert (Individual) certificates requires prior arrangement between HKPost and the Subscriber Organisation.

A CMMP User includes:

(a) Civil servants and contract staff employed by government direct;
(b) Agency / body-shop contract staff (including T-contract IT staff);
(c) Resident officers engaged under contract arrangement (e.g. outsourcing contract) other than (b) above.

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

CMMP user with a certificate of this class (g-Cert (Individual)) may use it on CMMP for the following purposes where the electronic message is not classified as a confidential email:

(a) (as a sender) to digitally sign an electronic message by attaching a cryptographic signature using the certificate;
(b) (as a sender) to prevent tampering of the electronic message by digitally sealing it;
(c) (as a recipient) to allow a sender to encrypt an electronic message using the public key of the recipient,
(d) (as a recipient) to decrypt electronic message when it is received; and
(e) (as a recipient) to acknowledge receipt of encrypted message by sending an acknowledgement with a digital signature added to it to confirm the recipient's identity .

g-Cert (Individual) certificates can only be used by CMMP 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 CMMP USER OF THE g-Cert (Individual) TO USE THE CERTIFICATE FOR ANY PURPOSE OTHER THAN THOSE STATED ABOVE WITHIN THE DESIGNATED APPLICATIONS REFERRED TO IN APPENDIX H.

1.3.4.1.2 g-Cert (Functional Unit) Certificates

A g-Cert (Functional Unit) is issued to CMMP functional unit at the request of the Requester acting on behalf of B/D/Os of the Government of Hong Kong SAR (the "Subscriber Organisation" as listed in Appendix E); and that g-Cert identifies the CMMP functional unit of a Subscriber Organisation whom that Subscriber Organisation has duly authorised the use of Private Key of that g-Cert (Functional Unit) issued to that Functional Unit. Offer of g-Cert (Functional Unit) certificates requires prior arrangement between HKPost and the Subscriber Organisation.

g-Cert (Functional Unit) is for use by functional units belonging to the relevant B/D/O.

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

Certificates of this class (g-Cert (Functional Unit)) are to be used in CMMP only:

(a) to digitally sign an electronic message by attaching a cryptographic signature using the certificate;
(b) to preventing tampering of the electronic message by digitally sealing it;
(c) to encrypt and decrypt electronic messages; and
(d) to acknowledge receipt of encrypted message by sending an acknowledgement with a digital signature added to it to confirm the receiving user's identity, which is the identity of this functional unit.

g-Cert (Functional Unit) certificates can only be used by CMMP functional units 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 FUNCTIONAL UNIT OF THE g-Cert (Functional Unit) TO USE THE CERTIFICATE FOR ANY PURPOSE OTHER THAN THOSE MENTIONED ABOVE WITHIN THE DESIGNATED APPLICATIONS REFERRED TO IN APPENDIX H.

1.3.5 Relying Parties

Relying Parties are entities that rely on any class or category of certificate issued by HKPost, including, but not limited to g-Cert for verifying digital signatures.

1.3.6 Other participants

HKPost may subcontract its obligations for performing some or all of the functions required by this CPS and the Subscriber Agreement provided that the subcontractor agrees to undertake to perform those functions and enters into a contract with HKPost to perform the services. In the event that such sub-contracting occurs, save in the case of negligence, acting out of scope of authorisation, fraud, criminal acts or other similar factors, HKPost shall remain liable for the performance of the CPS and the Subscriber Agreement as if such sub-contracting had not occurred.

As mentioned above, Certizen Limited and its sub-contractors (collectively known as the Contractor) are indeed one of the subcontractors appointed by HKPost.

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

systems and services as stipulated in this CPS. HKPost is and remains responsible for the activities of the Contractor in the performance or purported performance by the Contractor of the functions, power, rights and duties of HKPost.

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

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

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

g-Cert issued under this CPS are intended solely for secure electronic mail communications, including the digital signing and encryption of electronic mail. The digital signatures generated by the certificate are under no circumstances to be used for negotiation or conclusion of a contract or any legally binding agreement or any monetary transactions.

1.4.2 Prohibited Certificate Uses

g-Cert issued under this CPS shall not be used for purposes other than secure electronic mail communications, including but not limited to TLS authentication, code signing, or non-email document signing.

1.5 Policy Administration

1.5.1 Organisation Administering the Document

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

1.5.2 Contact Person

Subscribers may send their enquiries, suggestions or complaints by:

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

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

1.5.3 Person Determining CPS Suitability for the Policy

HKPost shall maintain this CPS in compliance with the Electronic Transactions Ordinance (Cap. 553) and relevant regulations of the Code of Practice for Recognized Certification Authorities ("Code of Practice") of Hong Kong.

1.5.4 CPS Approval Procedures

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

1.6 Definitions and Acronyms

Definitions and acronyms used in this CPS are provided in **Appendix A**.

2. Publication and Repository Responsibilities

2.1 Repositories

Under the Ordinance, HKPost maintains a publicly accessible Repository that contains information relevant to g-Cert issued under this CPS. The Repository includes accepted certificates, Certificate Revocation Lists (CRLs), the HKPost Public Key, a copy of this CPS, and other information related to g-Cert which reference this CPS HKPost shall as soon as possible publish and update the Repository regarding the relevant disclosed documents and disclosure records of the previously published documents and their amendments.

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

2.2 Publication of Certification Information

The HKPost Repository can be accessed at URLs as follows:

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

or alternatively

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

2.3 Time or Frequency of Publication

The Repository is available on a substantially 24 hours per day, 7 days per week basis, subject to scheduled maintenance of an average of 2 hours per week and any emergency maintenance. The Repository is updated promptly after each certificate is accepted by and issued to the Subscriber and any other applicable events such as update of certificate revocation list.

On top of other changes from time to time, HKPost reviews and updates this CPS at least every 365 days and makes appropriate changes so that HKPost operation remains accurate, transparent and complies with external requirements listed in the "*PREAMBLE*" section of this document. New or modified versions of this CPS is typically published within seven (7) days after its approval.

2.4 Access Controls on Repositories

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

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

3. Identification and Authentication

This section describes the identification, authentication, and mailbox validation requirements applicable to Applicants and Subscribers of g-Cert (Individual) and g-Cert (Functional Unit) certificates issued under this CPS.

3.1 Naming

g-Cert issued under this CPS identify Subscribers using Subject Names constructed in accordance with the naming rules and certificate profiles specified in **Appendix B**.

3.1.1 Types of Names

3.1.1.1 g-Cert (Individual) certificates

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

a) The email address of mailbox under the CMMP User's control in the Subject Alternative Name (SAN) extension;
b) The CMMP User's name as it appears on the documents to verify its identity;
c) The Subscriber Organisation's name as it is registered with the appropriate Hong Kong Government Department whose existence is recognized by the laws of Hong Kong SAR, or the official name of that Bureau or Department or Office where the Subscriber Organisation is a Bureau or Department or Office of the Government of Hong Kong SAR.

3.1.1.2 g-Cert (Functional Unit) certificates

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

a) The email address of mailbox under the CMMP User's control in the Subject Alternative Name (SAN) extension;
b) The Subscriber Organisation's name as it is registered with the appropriate Hong Kong Government Department whose existence is recognized by the laws of Hong Kong SAR, or the official name of that Bureau or Department or Office where the Subscriber Organisation is a Bureau or Department of Office of the Government of Hong Kong SAR.

3.1.1.3 The Requester, Business Administrator, B/D/O Administrator in CMMP

Although the Requester, Business Administrator and B/D/O Administrator of the Subscriber Organisation, who is assigned by B/D/O, is responsible for administering on behalf of the Subscriber Organisation the application for an g-Cert certificate in CMMP, that person will not be identified in the g-Cert.

3.1.2 Need for Names to be Meaningful

All Subject Names included in g-Cert under this CPS must be meaningful and use commonly understood semantics to enable determination of the identity of the Subscriber.

3.1.3 Anonymity or Pseudonymity of Subscribers

HKPost does not issue anonymous or pseudonymous certificates under this CPS.

3.1.4 Rules for Interpreting Names

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

3.1.5 Uniqueness of Names

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

3.1.6 Recognition, Authentication, and Role of Trademarks

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

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

3.2 Initial Identity Validation

For different staff categories as mentioned in 1.3.4.1 of this CPS, the Business Administrator role can be further defined into Business Administrator for different staff categories to take care of the different verification requirements:

Staff Category	Description
Civil servant or contract staff employed by government direct	The "Verify" step shall be conducted by a CMMP User who has the Business Administrator role for this staff category. This person is responsible to check the certificate holder's documents which contain the documentary evidence* against the personnel record kept in the Government.
Agency or body-shop contract staff (e.g. T-contract IT staff)	The "Verify" step shall be conducted by a CMMP User who has the Business Administrator role for this staff category. This person is responsible to check the certificate holder's documents which contain the documentary evidence* against the record kept in the agency or body-shop contract or related documents held by the B/D/O.
Resident officer engaged under contract arrangement	The "Verify" step shall be conducted by a CMMP User who has the Business Administrator role for this staff category. This person is responsible for checking the certificate holder's documents which contain the documentary evidence* against the record kept in the contract, agreement, order or other kind of legal documents used in the business relationship between the B/D/O and the outsourcer that can verify the identity of the certificate holder.

* documentary evidence can be Hong Kong Identity (HKID) Card, Passport information or other documents that B/D/O has been using for checking of identity

In case of doubt, HKPost may decline the g-Cert application.

3.2.1 Method to Prove Possession of Private Key

CMMP carries out the central key generation service on behalf of the Subscriber in a hardware security module ("HSM") hosted in a Trustworthy System and environment within the CMMP's premises to ensure that the Private Key is not tampered with, and generates and transmits 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 in a secure manner.

3.2.2 Authentication of Organisation Identity

Subscriber Organisations are bureaux, departments, or offices of the HKSAR Government. The identity of a Subscriber Organisation is established through its status as a recognised government entity and its participation in the CMMP.

Applications of g-Cert are submitted via CMMP by authorised roles designated by the Subscriber Organisation. The use of CMMP and the assignment of authorised roles provide assurance of the identity and authority of the Subscriber Organisation.

HKPost uses the following Registration Schemes:

a) GOVHK: For Government Entities

3.2.3 Authentication of Individual Identity

For g-Cert (Individual) certificates, CMMP relies on the prior authentication of individuals by the relevant Subscriber Organisation and on the assignment of authorised user roles within CMMP.

The use of CMMP user accounts and role assignment provides assurance that the individual associated with a g-Cert (Individual) certificate has been authenticated by the Subscriber Organisation. (BR Section 3.2.4.1(6))

3.2.4 Non-Verified Subscriber Information

HKPost verifies the subject elements and the Mailbox Field in the subject alternative name extension as defined in the S/MIME BR. Subscriber information that has not been verified in accordance with the S/MIME BR SHALL NOT be included in g-Cert certificates.

3.2.5 Validation of Authority and Mailbox Control

HKPost establishes authority over, or control of, the mailbox address associated with an g-Cert certificate as part of initial identity validation. HKPost uses the following validation method:

a) Validation of authority over mailbox via domain (S/MIME BR Section 3.2.2.1) HKPost may confirm that an Applicant or a Subscriber Organisation is authorised to act on behalf of the mailbox holder by validating control over the domain portion of the mailbox address. Where domain-based validation is performed, HKPost uses only the approved domain validation methods specified in Section 3.2.2.4.12 of the CA/Browser Forum Baseline Requirements for TLS Server Certificates.

For validation of mailbox authorization or control, any reused data, document, or completed validation has been obtained no more than 30 days prior to issuing the g-Cert.

3.2.6 Criteria for Interoperation

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

3.3 Identification and Authentication for Re-Key Requests

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

i) Replacement of a certificate, which is when some (or none) of the subject details have been changed after the application and the Subscriber may (or may not) wish to change the key associated with the new certificate;
ii) Renewal of a certificate, which is when the Subscriber wishes to extend the lifetime of an existing certificate and may also change the key associated with the certificate.

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

3.3.1 Identification and Authentication for Routine Re-Key

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

3.3.2 Identification and Authentication for Re-Key After Revocation

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

A Subscriber acting through the Requestor must undergo the initial registration process as described in Section 3.2.

3.4 Identification and Authentication for Revocation Requests

After receiving the revocation request from subscriber or through the RA to which the request for revocation was first submitted, HKPost shall validate the request and verify the justifications for revocation. The certificate will be revoked, which terminates the validity of the certificate permanently, upon receipt of the final confirmation of revocation from the Subscriber or through the RA to which the request for revocation was first submitted. Such final confirmation of revocation can be a system interface file, containing the certificate revocation data, submitted by CMMP to HKPCA through dedicated and secured network connections with TLS protocol.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

All first applications and applications of a new g-Cert following the revocation or expiration of a g-Cert will require the applicants to submit their applications in CMMP. The CMMP will complete and transmit the application to the HKPost.

4.1.1 Who Can Submit a Certificate Application

For g-Cert (Individual) and g-Cert (Functional Unit) certificates, applications are submitted by the Requester via the CMMP on behalf of the Applicant.

4.1.2 Enrolment Process and Responsibilities

Applicants for g-Cert must complete the enrolment process, which includes:

a) By submitting a g-Cert request electronically via CMMP, the Applicant authorises the publication of the g-Cert to any other person or in the Repository and accepts the g-Cert to be issued to the Applicant,
b) Pay any applicable subscription fees,
c) Generate the Private Key and public key.

By submitting a g-Cert request electronically via CMMP, the Applicant authorises the publication of the g-Cert to any other person or in the HKPost Repository and thus accepts the g-Cert to be issued to the Applicant.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

The documentation required for proving the identity of the Applicant is stipulated in Sections 3.2 of this CPS. Meanwhile, HKPost retrieves and processes the Certification Authority Authorisation record(s) ("CAA Record") in accordance with RFC 9495 prior to issuing a g-Cert. If a CAA Record exists that does not list HKPost's domain names, neither "eCert.gov.hk" nor "hongkongpost.gov.hk", as an authorised issuer domain name, the certificate application will not be proceeded. If no CAA Record exists for the domain name(s) to be identified in the certificate, HKPost considers that the Applicant allows HKPost to issue certificate for the domain name(s).

Validation of mailbox authorization

Following successful identity, authority, and mailbox validation as described in Section 3.2, HKPost proceeds with certificate application processing in accordance with the procedures set out in this Certification Practice Statement.

Verification on Certificate Information

Applicants can either verify the information on the certificate by browsing the certificate file or through HKPost CA Repository. Applicants should notify HKPost immediately of any incorrect information of the certificate.

Publication of g-Cert certificate

Under the Ordinance, HKPost shall publish promptly the accepted and issued g-Cert in the Repository (see Section 2). Applicants can either verify the information on the certificate by browsing the certificate file or through HKPost CA Repository. Applicants should notify HKPost immediately of any incorrect information of the certificate.

4.2.2 Approval or Rejection of Certificate Applications

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

4.2.3 Time to Process Certificate Applications

No stipulation.

4.3 Certificate Issuance

4.3.1 Following the identity verification process, CMMP will carry out the central key generation service on behalf of the Subscriber in a hardware security module ("HSM") hosted in a Trustworthy System and environment within the CMMP 's premises to ensure that the Private Key is not tampered with, and generate and transmit the Certificate Signing Request (CSR) containing the Public Key to HKPost. HKPost will generate the g-Cert certificates (with the Public Key included) of the respective CMMP Users / CMMP Functional Unit in a Trustworthy System and environment within HKPost's premises.

4.3.2 The g-Cert will then be delivered electronically to the CMMP User / CMMP Functional Unit via CMMP.

4.3.3 The CMMP agrees that it is fully accountable for the safe custody of the Private Key upon receipt of the g-Cert certificate and agree that they will be responsible for any consequences under any circumstances for the compromise of the Private Key.

4.3.4 All Private Keys stored in the HSM hosted in a Trustworthy System and environment within the CMMP'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.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Applicants can either verify the information on the certificate by browsing the certificate file or through HKPost CA Repository. Applicants should notify HKPost immediately of any incorrect information of the certificate.

4.4.2 Publication of the Certificate by the CA

All issued and accepted g-Certs will be published in the Repository under the Ordinance.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subscribers shall use g-Cert and corresponding Private Keys solely for secure electronic mail (S/MIME) purposes in accordance with this CPS and the CA/Browser Forum Baseline Requirements for S/MIME.

Subscriber Organisations are responsible for:

a) Acknowledging that they are undertaking an obligation to protect the confidentiality (i.e. keep it secret) and the integrity of the Private Key of the g-certs applied for by them using reasonable precautions to prevent its loss, disclosure, or unauthorised use, and that they are responsible for any consequences under any circumstances for the compromise of the Private Key.
b) Reporting any loss or compromise of their Private Key immediately to HKPost upon discovery of the loss or compromise (a compromise is a security violation in which Information is exposed to potential unauthorised access, such that unauthorised disclosure, alteration, or use of the Information may have occurred).
c) For the purpose of identity authentication, using the Private Key of an g-Cert only during its validity period.
d) authorised users have the Subscriber Organisation's authority to use, and in fact use, the certificate and associated Private Key solely for secure electronic mail (S/MIME) purposes in accordance with this CPS;
e) such certificates are used only for secure electronic mail (S/MIME) communications, including the encryption and decryption of electronic mail and, where applicable, the digital signing of electronic mail, in accordance with the CA/Browser Forum Baseline Requirements for S/MIME;
f) no attempt is made to use the Private Key relating to a g-Cert Certificate for any purposes other than secure electronic mail (S/MIME) communications as permitted under this CPS; and
g) reasonable precautions are taken by the authorised users to maintain the security of the Private Key.

4.5.2 Relying Party Public Key and Certificate Usage

Relying Parties relying upon g-Cert are responsible for:

a) Relying on such certificates only when the reliance is reasonable and in good faith in light of all the circumstances known to the Relying Party at the time of the reliance.
b) Before relying upon a certificate determining that the use of the certificate and any digital signature supported by it is appropriate for its purposes under this CPS.
c) Checking the status of the certificate on the certificate revocation list prior to reliance.
d) Performing all appropriate certificate path validation procedures.
e) After validity period of the certificate, only using its Public Key for signature verification.

4.6 Certificate Renewal

4.6.1 Circumstances for Renewal

Renewal of g-Cert is permitted prior to certificate expiry, subject to the requirements of this CPS.

4.6.2 Who May Request Renewal

The Requester of the Subscriber Organisation will need to submit the renewal request electronically via CMMP to HKPost and pay for appropriate subscription fees. The process of "Authentication of Individual Identity" as described under Section 3.2.3 will be conducted as if a new application is received.

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 requests for renewal via CMMP.

4.6.3 Processing Renewal Requests

4.6.3.1 Renewal of g-Cert Certificates

Where a certificate is issued or renewed under this CPS, the validity period shall not exceed the maximum validity period permitted under the CA/Browser Forum Baseline Requirements for S/MIME.

CMMP will notify Subscribers to renew the g-Cert 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 or revoked certificates.

The certificate validity of g-Cert (Individual) is one year. The validity period of the certificate for the certificate holder can be selected by B/D/O subject to their business needs.

The certificate validity of g-Cert (Functional Unit) is one year. The validity period of the certificate for the certificate holder can be selected by B/D/O subject to their business needs.

Upon certificate renewal, a new key pair of the Subscriber will be generated through CMMP's central key generation service. Upon certificate renewal, the terms and conditions of the original Subscriber Agreement will apply to the renewed certificate, except insofar as such terms are incompatible with the terms of the CPS current at the date of renewal. In the case of such incompatibility the terms of the current CPS will prevail. Applicants for renewal should read the terms of the CPS current at the date of renewal before submitting the renewal forms.

4.6.4 Notification of New Certificate Issuance to Subscriber

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

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Subscriber's conduct constituting acceptance of a renewal g-Cert is the same as listed in Section 4.4.1 of this CPS.

4.6.6 Publication of the Renewal Certificate by the CA

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

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

RAs may receive notification of a certificate's renewal if the RA was involved in the issuance process.

4.7 Certificate Re-Key

4.7.1 Circumstances for Certificate Re-Key

Re-keying a certificate consists of creating a new certificate with a new Public Key and serial number while keeping the subject information the same. Certificate re-key will ordinarily take

place as part of a certificate renewal process, or on HKPost's discretionary as part of a certificate replacement process.

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

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

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

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

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

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

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

4.8.1 Circumstances for Certificate Modification
No stipulation.

4.8.2 Who May Request Certificate Modification
No stipulation.

4.8.3 Processing Certificate Modification Requests
No stipulation.

4.8.4 Notification of New Certificate Issuance to Subscriber
No stipulation.

4.8.5 Conduct Constituting Acceptance of Modified Certificate
No stipulation.

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

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

4.9 Certificate Revocation and Suspension
Each Subscriber may make a request to revoke the certificate for which they are responsible under a Subscriber Agreement at any time for any reason by following the revocation procedure set out in this CPS. Suspension of a certificate is not applicable.

4.9.1 Circumstances for Revocation

4.9.1.1 The compromise of a HKPost Private Key will result in prompt revocation of the certificates issued under that Private Key. Procedures stipulated in the HKPost key compromise plan will be exercised to facilitate rapid revocation of all Subscriber certificates in the event of compromise of the HKPost Private Keys (see Section 5.7.3).

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

4.9.1.3 Each Subscriber **MUST** apply to B/D/O 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 g-Cert 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 CMMP User in the corresponding g-Cert is changed or becomes invalid.**

4.9.1.4 HKPost may revoke a certificate and HKP will whether by prior or retrospective notice notify the Subscriber by updating the certificate revocation list and by email, if a contact email address is available, of such 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 CMMP User identified in an g-Cert certificate has ceased to be an CMMP User of the Subscriber Organisation; or
h) knows or has reasonable cause to believe that the CMMP User identified in an g-Cert certificate has ceased to possess the Role in the Subscriber Organisation.

4.9.1.5 HKPost will revoke a g-Cert within 24 hours counting from any one of the events mentioned below:

1) the next working following from the day of receipt of the Subscriber requests in writing that HKPost revoke the g-Cert;
2) the next working following from the day of receipt of the Subscriber's notification to notify HKPost that the original Certificate Request was not authorized and does not retroactively grant authorization;

3) HKPost obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the g-Cert suffered a Key Compromise;
4) HKPost is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys);
5) HKPost obtains evidence that the validation of domain authorization or mailbox control for any Mailbox Address in the g-Cert should not be relied upon.

4.9.1.6 HKPost may revoke a g-Cert within 24 hours counting from any one of the following events and in any event will revoke a g-Cert within 5 days at the latest:

1) The g-Cert no longer complies with the requirements of Section 6.1.5 and Section 6.1.6 of the S/MIME BR;
2) HKPost obtains evidence that the g-Cert was misused;
3) HKPost is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement;
4) HKPost is made aware of any circumstance indicating that use of an email address or Fully-Qualified Domain Name in the g-Cert is no longer legally permitted (e.g., a court or arbitrator has revoked the right to use an email address or Domain Name, a relevant licensing or services agreement between the Subscriber has terminated, or the account holder has failed to maintain the active status of the email address or Domain Name);
5) HKPost is made aware of a material change in the information contained in the g-Cert;
6) HKPost is made aware that the g-Cert was not issued in accordance with the S/MIME BR or HKPost's CP and/or CPS;
7) HKPost determines or is made aware that any of the information appearing in the g-Cert is inaccurate;
8) HKPost's right to issue g-Cert under the S/MIME BR expires or is revoked or terminated, unless HKPost has made arrangements to continue maintaining the CRL or OCSP Repository;
9) Revocation is required by the HKPost's CP and/or CPS; or
10) HKPost is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed.

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

4.9.2 Who Can Request Revocation

A Requester should login the CMMP, complete and submit a request of certificate revocation in the CMMP for an Applicant of g-Cert (Individual) or a functional unit of g-Cert (Functional Unit).

Business Administrator should login the CMMP and approve the request within a pre-defined number of working day(s) set by B/D/O.

4.9.3 Procedure for Revocation Request

CMMP may provide an Application Interface (API) to receive a request of certificate revocation including workflow processing information by Requester and Business Administrator from B/D/O system through dedicated and secured network connections. The CMMP shall conduct the validation on the request and authority checking on workflow for Requester and Business Administrator according to the CMMP records.

The CMMP shall prepare a system interface file, containing the certificate revocation data. The interface file shall be submitted to HKPCA through dedicated and secured network connections with TLS protocol.

HKPCA will revoke the certificate, which terminates the validity of the certificate permanently. The information of all Certificates that have been revoked will be included in the Certificate Revocation List. HKPCA will publish the Certificate Revocation List in accordance with the schedule.

The CMMP shall receive system interface file, containing result of certificate revocation from HKPCA through dedicated and secured network connections with TLS protocol. Hence, the CMMP shall inactivate the corresponding g-Cert and notify all CMMP Users who have been involved in the process the completion of the request.

The information of all Certificates that have been revoked, including the reason code identifying the reason for the certificate revocation, will be included in the Certificate Revocation List (see Section 7.2).

4.9.4 Revocation Request Grace Period

The revocation request grace period ("Grace Period") means the period during which the Subscriber should make a revocation request but request outside the Grace Period may still be processed due to circumstances beyond the control of the Subscriber. Each Subscriber MUST apply to HKPost for the revocation of the certificate in accordance with the revocation procedures in this CPS immediately after the Subscriber's Private Key, or the media containing the Private Key corresponding to the Public Key contained in an g-Cert has been, or is suspected of having been, compromised or any change in the Information in the certificate provided by the Subscriber.

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

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

HKPost shall be under no liability to Relying Parties in respect of the transactions in the period between HKPost's decision to revoke a certificate (either in response to a request or otherwise)

and the appearance of the revocation status on the Certificate Revocation List, unless HKPost has failed to exercise reasonable skill and care and the Subscriber has failed to notify the Relying Party as required by these provisions. Any such liability is limited as set out elsewhere in this CPS.

4.9.5 Time within Which CA Must Process the Revocation Request
HKPost shall exercise reasonable endeavours to ensure that within 24 hours starting from the next working date of (1) receiving a revocation request or final confirmation of revocation from the Subscriber or (2) in the absence of such a request, the decision by HKPost to revoke the certificate, the revocation is posted to the Certificate Revocation List. However, a Certificate Revocation List is not immediately published in the directory for access by the public following each certificate revocation. Only when the next Certificate Revocation List is updated and published will it reflect the revoked status of the certificate. Certificate Revocation Lists are published 3 times daily and are archived for at least 7 years.

HKPost shall exercise reasonable endeavours to notify relevant Subscribers by updating the certificate revocation list, and by email, if a contact email address is available, within 24 hours following the revocation.

4.9.6 Revocation Checking Requirements for Relying Parties
Relying Parties before relying upon this certificate are responsible for checking the status of this certificate on the Certificate Revocation List prior to reliance.

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

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

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

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

4.9.8 Maximum Latency for CRLs
HKPost does not specify a separate maximum latency for CRLs beyond the update and publication arrangements set out in Sections 4.9.5, 4.9.7, and **Appendix C**. Generally, however, CRLs for g-Cert are posted automatically to the Repository within a commercially reasonable time after generation.

4.9.9 On-Line Revocation/Status Checking Availability
HKPost currently does not provide OCSP service for g-Cert.

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

4.9.11 Other Forms of Revocation Advertisements Available
No stipulation.

4.9.12 Special Requirements Related to Key Compromise
Any parties (including but not limited to Relying Parties and Application Software Suppliers) who can demonstrate a proof of the compromised private key of certificate, may submit the proof through the Compromised Key Reporting web page on the HKPost CA web site, with reason "key compromise" to HKPost. If HKPost discovers or suspects the compromise of a Private Key, it will use commercially reasonable efforts to notify the Subscriber, and will update the revocation reason code in a CRL to "key compromise" upon discovery of such reason or as required by Section 7.2 (a) of this CPS.

Reports to HKPost through the Compromised Key Reporting web page must include a proof of key compromise in either of the following formats : -

a) Certificate Signing Request (CSR) signed by the compromised Private Key with the Common Name "Proof of Key Compromise for HKPost" and verifiable by the Public Key of a valid certificate maintained in the Repository of HKPost; or
b) the Private Key itself.

4.9.13 Circumstances for Suspension
Suspension is not allowed for g-Cert.

4.9.14 Who Can Request Suspension
No stipulation.

4.9.15 Procedure for Suspension Request
No stipulation.

4.9.16 Limits on Suspension Period
No stipulation.

4.10 Certificate Status Services

4.10.1 Operational Characteristics
The information of all certificates that have been revoked, including the reason code identifying the reason for the certificate revocation, will be included in the Certificate Revocation List (see Section 7.2).

4.10.2 Service Availability
Certificate status services are available 24x7.

4.10.3 Operational Features
No stipulation.

4.11 End of Subscription
Under the following three conditions, certificate subscription for Subscribers will be terminated:

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

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

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

HKPost has clearly set out the requirements for certificate subscription termination, draw up specific workflow for certificate subscription termination and properly retain the records in accordance with the Retention Period for Archive specified in Section 5.5.2.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

No private key escrow process is planned for HKPost Private Keys and Subscribers' Private Keys in the g-Cert system used by HKPost.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5. Facility, Management, and Operational Controls

5.1 Physical Controls

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

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

The security control measures limit access to the hardware and software (including the CA server, workstations, and any external cryptographic hardware modules or tokens under HKPost's control) used in connection with providing the HKPost CA services. Access to such hardware and software is limited to those personnel performing in a trusted role as described in Section 5.2.1 of this CPS. Assess shall be under control and be monitored manually or by electronic means to prevent unauthorised intrusion at all times. The access control system has included the functions of check-in/check-out record and time-out alert, and such records shall be archived on a regular basis and shall be kept for at least 7 years.

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

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

5.1.5 Fire Prevention and Protection
A fire prevention plan and a fire suppression system have been established for the CA facility. Fire protective measures have complied with the requirements specified by Fire Services Department of Hong Kong. The computer room has been installed with automatic fire alarm system and fire extinguishing system. Two types of fire detectors have been installed for detecting temperature and smoke. The fire alarm system and the fire extinguishing system have been linked together.

5.1.6 Media Storage
Media storage and disposition processes have been developed and are in place. For paper documents including Subscriber Agreements and photocopies of identity confirmation

documents, they are maintained by HKPost, the Contractor or its RAs in a secure fashion. Only authorised personnel are permitted access to the paper records.

5.1.7 Waste Disposal

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

5.1.8 Off-site Backup

HKPost has established backup systems for critical systems (including HKPost CA System) and data (including any sensitive information and audit data). Off-site backup measures have been implemented for critical systems and data to ensure these systems and data are stored in secure facilities against theft, damage and media storage deterioration (see Section 5.7.4).

5.2 Procedural Controls

5.2.1 Trusted Roles

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

5.2.2 Number of Personnel Needed for Each Task

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

5.2.3 Identification and Authentication of Each Role

Based on the nature of operations as well as the rights for their positions, the personnel working in trusted positions shall be granted with the rights to access systems and physical environments, and shall adopt appropriate access control techniques to maintain a complete record of all sensitive operations performed by such personnel.

5.2.4 Roles requiring Segregation of Duties

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

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

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

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

5.3.2 Background Check Procedures

HKPost conducts and/or requires the Contractor and RAs to conduct investigations of personnel who serve in trusted roles (prior to their employment and periodically thereafter as necessary and require the personnel to present their valid proof of identity) to verify such employee's trustworthiness and competence in accordance with the requirements of this CPS and HKPost's personnel policies. Personnel who fail an initial or periodic investigation are not permitted to serve or to continue to serve in a trusted role. Also, relevant security provisions have been incorporated in staff contract and the personnel must agree and sign the contract before their employment.

5.3.3 Training Requirements

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

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

5.3.4 Retraining Frequency and Requirements

HKPost, the Contractor and the RAs shall use their reasonable endeavours to provide appropriate and sufficient training for their staff (at least once a year for those holding core positions) to ensure their capabilities in carrying their duties as well as effective implementation and compliance with security policies.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorised Actions

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

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

5.3.7 Independent Contractor Requirements

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

5.3.8 Documentation Supplied to Personnel

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

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

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

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

CA certificate and key lifecycle events, including:

- Key generation, backup, storage, recovery, archival, and destruction;
- Certificate requests, renewal, and re-key requests, and revocation;
- Approval and rejection of certificate requests;
- Cryptographic device lifecycle management events;
- Generation of CRLs; and
- Introduction of new Certificate Profiles and retirement of existing Certificate Profiles.

Subscriber Certificate lifecycle management events, including:

Certificate requests, renewal, and re-key requests, and revocation;

- All verification activities stipulated in this CPS;
- Approval and rejection of certificate requests;
- Issuance of Certificates; and
- Generation of CRLs.

Security events, including:

- Successful and unsuccessful PKI system access attempts;
- PKI and security system actions performed;
- Security profile changes;
- Installation, update and removal of software on a certificate system;
- System crashes, hardware failures, and other anomalies;
- Firewall and router activities; and
- Entries to and exits from the CA facility.

Log records MUST include the following elements:

a) Date and time of event;
b) Identity of the person making the journal record; and

c) Description of the event.

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

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

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

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

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

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

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

5.5 Records Archival

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

a) System equipment configuration files;
b) Results of assessments and/or review for accreditation of the equipment (if conducted);
c) Certification Practice Statement and its modifications or updates;
d) Contractual agreements to which HKPost is bound;
e) All certificates and CRLs as issued or published;
f) Periodic event logs;
g) Other data necessary for verifying archive contents;
h) Documentations of the establishment and upgrading of certificate system;
i) Documentations supporting certificate application, information on the approval and rejection of certificate services, and certificate subscriber agreements;
j) Audit records;

k) Particulars of staff, including but not limited to information on their background, employment and training; and
l) Documentations of external or internal assessments.

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

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

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

5.5.5 Requirements for Time-Stamping of Records
Archived Information is marked with the date at which the archive item was created. HKPost utilizes controls to prevent the unauthorised manipulation of the system clocks.

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

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

5.6 Key Changeover
The lifespan of the HKPost CA and g-Cert root keys and certificates created by HKPost (See **Appendix G**) for the purpose of certifying certificates issued under this CPS is no more than 25 years. HKPost CA keys and certificates will be renewed at least 3 months before their certificates expire. Upon renewal of a root key, the associated root certificate will be published in HKPost web site http://www.eCert.gov.hk for public access. The original root keys will be kept for a minimum period as specified in Section 5.5.2 for verification of any signatures generated by the original root keys. HKPost shall ensure safe and smooth transition of the entire process, with a view to minimizing the adverse effects on Subscribers and Relying Parties.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures
HKPost maintains incident handling procedures to guide personnel in response to security incidents, natural disasters, and similar events that may give rise to system compromise. To maintain the integrity of certificate services, HKPost implements, documents, and periodically tests appropriate contingency and disaster recovery plans and procedures.

HKPost maintains a comprehensive and actionable plan for mass revocation events, performs annual testing of this plan, and incorporates lessons learned into this plan in order to continually improve preparedness over time.

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

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

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

5.7.3 Entity Private Key Compromise Procedures

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

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

In the event of key compromise or disaster where a HKPost Private Key for the issuance of g-Cert under this CPS has been compromised or corrupted and cannot be recovered, HKPost shall 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 issued with new certificates. In case of revocation requests for the HKPost CA root certificate, HKPost shall only proceed subject to the confirmation of the Commissioner for Digital Policy.

5.7.4 Business Continuity Capabilities after a Disaster

A managed process, including daily backup of essential business information and CA system data and proper backup of CA system software, is in place for maintaining business continuity plans to protect critical business processes from the effect of major failures or disasters. Business continuity plans exist to enable the complete recovery of all HKPost CA services. This incorporates a tested independent disaster recovery site which is currently located at least 10km from the primary CA operational site within the territory of Hong Kong Special Administrative

Region. The business continuity plans are reviewed and drilled annually. All personnel involved in the business continuity plans must participate in regular drilling exercises and record the drilling procedures and results.

HKPost shall promptly notify the 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.

5.8 CA or RA 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 shall properly archive the CA Records including certificates issued, root certificates, Certification Practice Statements and Certificate Revocation Lists for 7 years after the date of service termination.

In the event that the RA is terminated under RA agreement or under CA termination as stated above or the RA's authority to act on behalf of HKPost is withdrawn, the g-Certs applied through the RA will remain in effect in accordance with their terms and validity.

6. Technical Security Controls

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

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

HKPost generates the root key pairs for issuing certificates that conform to this CPS.

Signing key generation, storage, and signing operations performed by HKPost are conducted within a hardware cryptographic module that is rated to at least FIPS 140-2 Level 3.

For root CA and Sub CA key pairs, HKPost shall;

a) prepare and follow a key generation script,
b) have a qualified auditor witness the CA key pair generation process or record a video of the entire CA key pair generation process, and
c) have a qualified auditor issue a report opining that HKPost followed its root CA key ceremony script during its key and certificate generation process and the controls used to ensure the integrity and confidentiality of the key pair.

6.1.2 Private Key Delivery to Subscriber

Key pairs for g-Cert will be generated under the central key generation by CMMP on behalf of the Applicant/Subscriber.

6.1.3 Public Key Delivery to Certificate Issuer

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 CA Public Key Delivery to Relying Parties

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

6.1.5 Key Sizes

The HKPost signing key pair is 4096-bit RSA. Subscriber key pair is 2048-bit RSA.

6.1.6 Public Key Parameters Generation and Quality Checking

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

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

Keys used in g-Cert are used for the purposes of conducting enciphered electronic communications and other purposes as specified in section 1.3.4.1 above only. If digital signature Key Usage is enabled in the g-Cert (referred to in **Appendix B**), the digital signatures supported by the g-Cert are to be used only for providing authentication, data integrity, and

non-repudiation by using asymmetric cryptography. 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 and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls
The cryptographic devices used by HKPost are rated to at least FIPS 140-2 Level 3.

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

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

6.2.4 Private Key Backup
Each HKPost Private Key is backed up by encrypting and storing it in devices which conform to FIPS 140-2 Level 3 security standard. Backup of the HKPost Private Key is performed in a manner that requires more than one person to complete. The backup Private Keys must be activated by more than one person. No other Private Keys are backed-up.

6.2.5 Private Key Archival
All Private Keys will not be archived.

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

6.2.7 Private Key Storage on Cryptographic Module
HKPost Private Keys are created in a crypto module validated to at least FIPS 140-2 Level 3.

6.2.8 Method of Activating Private Key
Details concerning method of activating private key are found in Section 6.2.2.

6.2.9 Method of Deactivating Private Key
Details concerning method of deactivating private key are found in Section 6.2.2.

6.2.10 Method of Destroying Private Key
HKPost CA root keys will be used for no more than 25 years (see also Section 5.6). All HKPost key generation, key destruction, key storage, and certificate revocation list signing operations are performed in a hardware cryptographic module. Archival of HKPost Public Keys is performed as specified in Section 5.5.

6.2.11 Cryptographic Module Rating
Details concerning cryptographic module rating can be found in Section 6.2.1 of this CPS.

6.3 Other Aspects of Key Pair Management

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

HKPost CA root keys will be used for no more than 25 years (see also Section 5.6). All HKPost key generation, key destruction, key storage, and certificate revocation list signing operations are performed in a hardware cryptographic module. Archival of HKPost Public Keys is performed as specified in Section 5.5.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods
HKPost CA root keys will be used for no more than 25 years (see also Section 5.6). All HKPost key generation, key destruction, key storage, and certificate revocation list signing operations are performed in a hardware cryptographic module. Archival of HKPost Public Keys is performed as specified in Section 5.5.

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

Certificates issued under this CPS within the subscription period may be valid for a period different from the respective validity period listed above (see Section 4.6). The validity period of an g-Cert is specified in the certificate itself. Format of certificates issued under this CPS is in **Appendix B**.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation
HKPost Private Keys are stored in tamper-proof hardware cryptographic devices. HKPost implements multi-person control (2 out of 3 multi-person control) over the activation, usage, deactivation of HKPost Private Keys.

6.4.2 Activation Data Protection
HKPost Private Keys are stored in tamper-proof hardware cryptographic devices. HKPost implements multi-person control (2 out of 3 multi-person control) over the activation, usage, deactivation of HKPost Private Keys.

6.4.3 Other Aspects of Activation Data
No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements
HKPost implements multi-person control over the life cycle of activation data such as PINs and passwords for accessing the CA systems. Security procedures are in place to prevent and detect unauthorised access, modification, or compromise of the CA systems, in order to ensure the security and reliability of the CA systems which are hosting software, data and documents. With these procedures, the CA systems are protected from unauthorised internal or external access. Such security controls are subject to compliance assessment as specified in Section 8. HKPost implements stringent management mechanism to control and monitor the operating systems, in order to prevent unauthorised modification. When processing disposal of waste devices, HKPost will exercise reasonable endeavours to erase their storage with confirmation for which may contain information related to the security of g-Cert service.

6.5.2 Computer Security Rating
No stipulation.

6.6 Life Cycle Technical Controls

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

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

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

6.6.3 Life Cycle Security Controls
No stipulation.

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

HKPost shall conduct vulnerability scans at least once a quarter and penetration tests at least annually. All identified vulnerabilities shall be remediated promptly, typically within one month of patch release. Risk assessments shall be performed to determine appropriate mitigation strategies and timelines, with results documented. If remediation within one month is not feasible, HKPost shall assess the associated risks, create and implement a documented mitigation plan.

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

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

Certificates referred to in this CPS contain the Public Key used for confirming the identity of the sender of an electronic message and verifying the integrity of such messages, i.e., the Public Key used to verify a Digital Signature. A summary of the features of the g-Cert certificates is in **Appendix D**.

HKPost CA system shall generate non-sequential certificate serial numbers greater than zero (0) containing at least 64 bits of output from a CSPRNG.

7.1.1 Version Number(s)

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

7.1.2 Certificate Extensions

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

7.1.3 Algorithm Object Identifiers

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

7.1.4 Name Forms

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

7.1.5 Name Constraints

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

7.1.6 Certificate Policy Object Identifier

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

7.1.7 Usage of Policy Constraints Extension

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

7.1.8 Policy Qualifiers Syntax and Semantics

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

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

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

7.2 CRL Profile

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

When an g-Cert is revoked for one of the reasons below, the specified revocation reason code must be included in the reason code extension of the CRL entry corresponding to the certificate.

When the revocation reason code is not one of the following, then the reason code extension must not be provided:

Revocation reason	**Revocation reason code (CRLReason as specified in RFC5280)**
Key compromise	1 = keyCompromise
Privilege withdrawn	9 = privilegeWithdrawn (The revocation reason code "privilegeWithdrawn" does not need to be made available to the certificate subscriber as a revocation reason option, because the use of this revocation reason code is determined by the CA operator and not the subscriber.)
Cessation of operation	5 = cessationOfOperation
Affiliation changed	3 = affiliationChanged
Superseded	4 = superseded

The following is a description of each of these reason codes and circumstances where HKPost CA or a Subscriber will be obligated to use it for their revocation circumstances:

a) Revocation reason code (1) "keyCompromise"

The revocation reason code "keyCompromise" will be used when one or more of the following occurs:

- HKPost CA obtains verifiable evidence that the certificate subscriber's private key corresponding to the public key in the certificate suffered a key compromise; or
- HKPost CA is made aware of a demonstrated or proven method that exposes the certificate subscriber's private key to compromise; or
- There is clear evidence that the specific method used to generate the private key was flawed; or
- HKPost CA is made aware of a demonstrated or proven method that can easily compute the certificate subscriber's private key based on the public key in the certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys); or
- the certificate subscriber requests that HKPost CA revokes the certificate for this reason, with the scope of revocation being described below.

If anyone requesting revocation for "keyCompromise" has previously demonstrated or can currently demonstrate possession of the private key of the certificate through the Compromised Key Reporting web page on the HKPost CA web site as set out in Section 4.9.12 of this CPS, then HKPost CA will revoke all instances of that key across all subscribers.

If the certificate subscriber requests that HKPost CA revokes the certificate for "keyCompromise", and has not previously demonstrated and cannot currently demonstrate possession of the associated private key of that certificate, HKPost CA may revoke all certificates associated with that subscriber that contain that public key.

When HKPost CA obtains verifiable evidence of private key compromise for a certificate whose CRL entry does not contain a reason code extension or has a reason code extension with a non-"keyCompromise" reason, HKPost CA may update the CRL entry to enter "keyCompromise" as the revocation reason code in the reason code extension. Additionally, HKPost CA may

update the revocation date in a CRL entry when it is determined that the private key of the certificate was compromised prior to the revocation date that is indicated in the CRL entry for that certificate.

(Note: Backdating the revocation date field is an exception to best practice described in Section 5.3.2 of RFC 5280; however, this CPS specifies the use of the revocation date field to support Application Software Suppliers where the revocation date field is processed as the date when the certificate is first considered to be compromised.)

Otherwise, the "keyCompromise" revocation reason code must not be used.

b) Revocation reason code (9) "privilegeWithdrawn"

The revocation reason code "privilegeWithdrawn" is intended to be used when there has been a subscriber-side infraction that has not resulted in "keyCompromise", such as the certificate subscriber provided misleading information in their certificate request or has not upheld their material obligations under the subscriber agreement or terms of use.

Unless the "keyCompromise" revocation reason code is being used, the revocation reason code "privilegeWithdrawn" must be used when:

- HKPost CA obtains evidence that the certificate was misused; or
- HKPost CA is made aware that the certificate subscriber has violated one or more of its material obligations under the subscriber agreement or terms of use; or
- HKPost CA is made aware that an g-Cert has been used to authenticate a fraudulently misleading subordinate fully-qualified domain name; or
- HKPost CA is made aware of a material change in the information contained in the certificate; or
- HKPost CA determines or is made aware that any of the information appearing in the certificate is inaccurate; or
- HKPost CA is made aware that the original certificate request was not authorized and that the Subscriber does not retroactively grant authorization.

Otherwise, the "privilegeWithdrawn" revocation reason code must not be used.

c) Revocation reason code (5) "cessationOfOperation"

The revocation reason code "cessationOfOperation" is intended to be used when the website with the certificate is shut down prior to the expiration of the certificate, or if the subscriber no longer owns or controls the domain name in the certificate. This revocation reason code is intended to be used in the following circumstances:

- the certificate subscriber no longer controls, or is no longer authorized to use, all of the domain names in the certificate; or
- the certificate subscriber will no longer be using the certificate because they are discontinuing their website; or
- HKPost CA is made aware of any circumstance indicating that use of a fully-qualified domain name in the certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a domain name registrant's right to use the domain name, a relevant

licensing or services agreement between the domain name registrant and the applicant has terminated, or the domain name registrant has failed to renew the domain name).

Unless the "keyCompromise" revocation reason code is being used, the revocation reason code "cessationOfOperation" must be used when:

- the certificate subscriber has requested that their certificate be revoked for this reason; or
- HKPost CA received verifiable evidence that the certificate subscriber no longer controls, or is no longer authorized to use, all of the domain names in the certificate.

Otherwise, the "cessationOfOperation" revocation reason code must not be used.

d) Revocation reason code (3) "affiliationChanged"

The revocation reason code "affiliationChanged" is intended to be used to indicate that the subject's name or other subject identity information in the certificate has changed, but there is no cause to suspect that the certificate's private key has been compromised.

Unless the "keyCompromise" revocation reason code is being used, the revocation reason code "affiliationChanged" will be used when:

- the certificate subscriber has requested that the certificate be revoked for this reason; or
- HKPost CA replaced the certificate due to changes in the certificate's subject information and the CA has not replaced the certificate for the other reasons: "keyCompromise", "superseded", "cessationOfOperation", or "privilegeWithdrawn".

Otherwise, the "affiliationChanged" revocation reason code must not be used.

e) Revocation reason code (4) "superseded"

The revocation reason code "superseded" is intended to be used to indicate when:

- the certificate subscriber has requested a new certificate to replace an existing certificate; or
- HKPost CA obtains reasonable evidence that the validation of domain authorization or control for any fully-qualified domain name in the certificate should not be relied upon; or
- HKPost CA revoked the certificate for compliance reasons such as the certificate does not comply with this CPS, the CA/Browser Forum's Baseline Requirements, or the certificate policies of major root certificate programs (such as Mozilla Root Store Policy).

Unless the "keyCompromise" revocation reason code is being used, the revocation reason code "superseded" must be used when:

- the certificate subscriber has requested that their certificate be revoked for this reason; or

- HKPost CA revoked the certificate due to domain authorization or compliance issues other than those related to “keyCompromise” or “privilegeWithdrawn”.

Otherwise, the “superseded” revocation reason code must not be used.

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

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

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

7.3 OCSP Profile
No stipulation.

7.3.1 Version Number(s)
No stipulation.

7.3.2 OCSP Extensions
No stipulation.

8. Compliance Audit and Other Assessments

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

8.1 Frequency and Circumstances of Assessment

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

8.2 Identity/Qualifications of Assessor

Qualification of the independent external auditor conducting compliance assessments are in accordance with the requirements set out in the Ordinance and the Code of Practice for Recognized Certification Authorities. In addition, any WebTrust auditor engaged must satisfy the requirements set forth in the latest available S/MIME BR.

8.3 Assessor's Relationship to Assessed Entity

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

8.4 Topics Covered by Assessment

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

8.5 Actions Taken as a Result of Deficiency

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

8.6 Communications of Results

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

8.7 Self-Audits

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

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees
The subscription fee shall be paid by g-Cert subscribers unless waived by HKPost. For details of the fees charged in respect of g-Cert certificates, please see **Appendix H**. HKPost reserves its absolute right to review and determine the subscription fee from time to time and will notify the Subscribers and the public at the HKPost web site http://www.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 g-Cert subscribers.

9.1.2 Certificate Access Fees
HKPost may charge a reasonable fee for direct access to its certificate databases.

9.1.3 Revocation or Status Information Access Fees
HKPost does not charge a certificate revocation fee or a fee for checking the validity status of an issued certificate using a CRL.

9.1.4 Fees for Other Services
Subject to review from HKPost from time to time.

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

9.2 Financial Responsibility

9.2.1 Insurance Coverage
HKPost maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage. Moreover, the insurance policy also covers the potential or actual liabilities and claims against Reliance Limit on the certificates pursuant to the provisions of ETO.

9.2.2 Other Assets
No stipulation.

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

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information
Information about Subscribers that is submitted as part of an application for a g-Cert under this CPS will be used only for the purposes collected and is kept confidential except for the name of the Subscriber, name of the CMMP user, and for other information which is to the extent necessary for HKPost or the Contractor to perform HKPost's obligations under this CPS.

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

9.3.3 Responsibility to Protect Confidential Information
HKPost shall ensure that the restrictions in this subsection will be adhered to by itself and any persons of HKPost, the Contractor, RAs and any HKPost subcontractors, who have access to any record, book, register, correspondence, information, document or other material in performing tasks related to HKPost's system of issuing, revoking and publishing g-Certs shall not disclose or permit or suffer to be disclosed any information relating to another person as contained in such record, book, register, correspondence, information, document or other material to any other person.

Any information identified as confidential including those mentioned in section 9.3.1 above will not be released without the prior consent of the Subscriber except when required by a court-issued subpoena or order, or when otherwise required by the laws of Hong Kong SAR. HKPost is specifically precluded from releasing lists of Subscribers or Subscriber Information (except for the release of compiled data which is not traceable to an individual Subscriber) unless required by a court-issued subpoena or order, or when otherwise required by the laws of Hong Kong SAR.

9.4 Privacy of Personal Information

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

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

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

9.4.4 Responsibility to Protect Private Information
HKPost shall ensure that the restrictions in this subsection will be adhered to by itself and any persons of HKPost, the Contractor, RAs and any HKPost subcontractors who have access to any record, book, register, correspondence, information, document or other material in

performing tasks related to HKPost's system of issuing, revoking and publishing g-Certs shall not disclose or permit or suffer to be disclosed any information relating to another person as contained in such record, book, register, correspondence, information, document or other material to any other person.

9.4.5 Notice and Consent to Use Private Information
Information about Subscribers that is submitted as part of an application for an g-Cert under this CPS will be used only for the purposes collected and is kept confidential except to the extent necessary for HKPost or the Contractor to perform HKPost's obligations under this CPS.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process
Any information identified as confidential including those mentioned in section 9.3.1 above will not be released without the prior consent of the Subscriber except when required by a court-issued subpoena or order, or when otherwise required by the laws of Hong Kong SAR. HKPost is specifically precluded from releasing lists of Subscribers or Subscriber Information (except for the release of compiled data which is not traceable to an individual Subscriber) unless required by a court-issued subpoena or order, or when otherwise required by the laws of Hong Kong SAR.

9.4.7 Other Information Disclosure Circumstances
No stipulation.

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

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

9.6 Representations and Warranties

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

By issuing a certificate that refers to this CPS, HKPost represents to Relying Parties who act in accordance with Section 9.6.4 and other relevant sections of this CPS, that HKPost has issued the certificate in accordance with this CPS. By publishing a certificate that refers to this CPS, HKPost represents to Relying Parties who act in accordance with Section 9.6.4 and other relevant sections of this CPS that HKPost has done the checking as mentioned in this CPS (including section 3.2) to verify that Applicant for the certificate is indeed the Subscriber Organisation identified in it.

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

9.6.2 RA Representations and Warranties

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

RAs carry out on HKPost's behalf HKPost's obligations and duties in these matters. RAs have the authority to act on behalf of HKPost to enforce the terms of the Subscriber Agreements (unless and until that authority is withdrawn and Subscribers duly notified of any such withdrawal).

9.6.3 Subscriber Representations and Warranties

Each Subscriber Organisation (represented by a Requester) must sign, or confirm its acceptance of, an agreement (in the terms specified in this CPS) which includes a term by which the Subscriber Organisation agrees that by accepting a certificate issued under this CPS, the Subscriber Organisation 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) Designated Applications effectuated using the private key corresponding to the public key included in the certificate are the acts of the CMMP User affiliated with the Subscriber Organisation as mentioned in section 1.3.4.1.1 above or the acts of the functional units mentioned in section 1.3.4.1.2 above and that the certificate has been accepted and is properly operational at the time throughout the validity of the certificate;
b) All Information and representations made by the Subscriber Organisation included in the certificate are true;
c) The Certificate is used exclusively for authorised and legal purposes consistent with this CPS;
d) The Subscriber Organisation will ensure that the use the certificate be confined to Designated Applications stipulated in **Appendix H**;
e) The Subscriber Organisation agrees with the terms and conditions of this CPS and other agreements and policy statement of HKPost;
f) The Subscriber Organisation has authorised CMMP to access the Subscriber Organisation's Private Key of the Certificate in Designated Applications stipulated in **Appendix H**;
g) All information supplied does not infringe or violate in any way the trademarks, service marks, trade name, company name, or other intellectual property rights of any third party upon issuance, acceptance, throughout the validity of the Certificate.

Subscribers are responsible for:

a) Completing the application procedures properly and signing, or confirming acceptance of, a Subscriber Agreement by the Authorised Representative in the appropriate form and performing the obligations placed upon them by that Agreement, and ensuring accuracy of representations in certificate application.
b) Accurately following the procedures specified in this CPS as to the end of certificate subscription.
c) Notifying HKPost immediately from time to time of any change in the appointment

and information of the CMMP user of g-Cert.

d) Notifying HKPost immediately of any fact which may give rise to HKPost, upon the grounds set out in Section 4 of this CPS, having the right to revoke the certificate for which that Subscriber is responsible.
e) Not using a certificate on becoming aware of any ground upon which HKPost could revoke it under the terms of the CPS, or after the Subscriber has made a revocation request or been notified by HKPost of HKPost's intention to revoke the certificate under the terms of this CPS.
f) Upon becoming so aware of any ground upon which HKPost could revoke the certificate, or upon the Subscriber making a revocation request or upon being notified by HKPost of its intention to revoke the certificate, immediately notifying Relying Parties in any transaction that remains to be completed at the time, that the certificate used in that transaction is liable to be revoked (either by HKPost or at the Applicant's or Subscriber's request) and stating in clear terms that, as this is the case, the Relying Parties should not rely upon the certificate in respect of the transaction.
g) Acknowledging that by submitting an g-Cert application form, they authorise the publication of the g-Cert to any other person or in the HKPost's Repository including the name of the CMMP user or the Subscriber Organisation.
h) For the purpose of identity authentication, using the Private Key of an g-Cert only during its validity period.

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

9.6.4 Relying Party Representations and Warranties

Relying Parties relying upon g-Cert are responsible for:

a) Relying on such certificates only when the reliance is reasonable and in good faith in light of all the circumstances known to the Relying Party at the time of the reliance.
b) Before relying upon a certificate determining that the use of the certificate and any digital signature supported by it is appropriate for its purposes under this CPS.
c) Checking the status of the certificate on the certificate revocation list whenever applicable, prior to reliance.
d) Performing all appropriate certificate path validation procedures.
e) After validity period of the certificate, only using its Public Key for signature verification.

9.6.5 Representations and Warranties of Other Participants

The Contractor is responsible 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. Save in the case of negligence, acting out of scope of authorisation, fraud, criminal acts or other similar factors, HKPost is and remains responsible for the activities of the Contractor in the performance or purported performance by the Contractor of the functions, power, rights and duties of HKPost.

9.6.5.1 CMMP Obligations

CMMP is assigned the following functions:

a) Defining user role "Requester" in CMMP so that B/D/O can assign staff to act as "Requester" for raising requests of certification, certificate renewal or certificate revocation on behalf of the CMMP User (the Applicant);
b) Defining user role "Business Administrator" in CMMP so that B/D/O can assign staff as RA for verifying the identity of the Applicant and approving the requests of certificate application, renewal and revocation in the CMMP;
c) Ensuring a CMMP User could not take up the role of "Business Administrator" and "the Requester" at the same time for a request for segregation of duties;
d) Defining and providing approval workflows acted on by different user roles in CMMP ("Requester", "Business Administrator") to conduct the corresponding tasks (submit request, verify and approve request) for the process of certificate application, renewal and revocation;
e) Generating and submitting certificate signing requests (CSR) on behalf of the Applicant to HKPost containing information in relation to the CMMP user or functional unit that matches with the information known to the CMMP at time of submission, together with the Applicant's confirmation on the Subscriber's terms and conditions;
f) Accepting the issued g-Cert from HKPost in a secure manner on behalf of the Applicant;
g) Ensuring that the generation of the Key Pair and its storage in a hardware security module ("HSM") of the CMMP;
h) Ensuring the safe custody of the Subscriber's Key Pair;
i) Ensuring that the g-Cert is only used for the Designated Applications specified in **Appendix H**;
j) Ensuring that the use by a CMMP user or functional unit of a g-Cert certificate for purposes other than the Designated Applications in Appendix H will not be permitted;
k) Ensuring that only the CMMP user and / or the functional unit specified in the g-Cert can make use of the Private Key to generate digital signature for the relevant Designated Application;
l) Verifying the identity of the CMMP user or the functional unit, before latter is permitted using its g-Cert in Designated Application;
m) Quoting the CMMP user's information through the use of a unique identity number assigned, that must uniquely reference to the CMMP user's evidence of identity, for submission of g-Cert application; and
n) Each time a g-Cert issued is used in a Designated Application, ensuring that the g-Cert has not expired or revoked based on the information as shown in the Repository and the CRL. Where g-Cert is expired or revoked, ensuring that the Designated Application will not be processed or completed using such g-Cert;

9.6.5.2 B/D/O Obligations

In addition to its duties as Subscriber, B/D/O are responsible for:

a) Assigning "Business Administrator" to act as the RA for verifying the identity of the Applicant and approving the requests of certificate application, renewal and revocation via the "Business Administrator" in CMMP;
b) Keeping of documentation evidence on the verification of identity of the applicants undertaken by "Business Administrator" role;

c) Assigning "Requester" for raising request of certificate application, renewal or revocation;
d) Ensuring the "Requester" complete the application procedures properly and confirm acceptance of the Subscriber terms and conditions on behalf of the Applicant;
e) Ensuring the g-Cert is used properly for Designated Applications in Appendix H; and
f) Ensuring the "Business Administrator" approve the request of certificate revocation within the number of working day(s) pre-defined by B/D/O;

9.7 Disclaimers of Warranties

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

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

This means, for example, that provided that the HKPost, the Contractor or the RA acting on HKPost's behalf has exercised a reasonable degree of skill and care, HKPost, Hong Kong Post Office, the Contractor and any such RA will not be liable for any loss to a Subscriber or Relying Party caused by their reliance upon a false or forged Digital Signature supported by another Subscriber's Recognized Certificate issued by HKPost.

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

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

9.8 Limitations of Liability

Each Subscriber and Relying Party must agree that it is reasonable for HKPost to limit its liabilities as set out in this CPS and (for the Subscriber) also in the Subscription Agreement. Save in the case of any negligence or fraud or acting outside the permitted scope of authority or other similar circumstances ("excepted situations"), all acts and omissions of the RA or the Contractor shall be deemed as acts and omissions of HKPost and the disclaimer and Reliance Limit shall equally apply in such cases. Even under excepted situations, to the extent legally possible, each of HKPost, the RA and the Contractor shall rely on the disclaimer and Reliance Limit set out in this Section 9.8.

In the event of:

a) HKPost's breach of this CPS or the Subscriber Agreement;
b) HKPost's breach of any duty of care; and in particular its duty under the Subscriber Agreement to exercise reasonable skill and care and/or duties that may arise to a Subscriber or Relying Party when any certificate issued by HKPost under the PKI is relied upon or used by a Subscriber or Relying Party or anyone else or otherwise howsoever; or
c) a loss caused by reliance on any information that HKPost is required to confirm according to this CPS and the code of practice; and which is misrepresented on that certificate or in a repository

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

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

Subject to the exceptions that appear below, in the event of:

a) HKPost's breach of this CPS or (applicable to the Subscriber only) the Subscriber Agreement;
b) HKPost's breach of any duty of care, and in particular, under this CPS or in law to exercise reasonable skill and care and/or any duties that may be owed to a Subscriber or Relying Party because 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; or
c) a loss caused by reliance on any information that HKPost is required to confirm according to this CPS and the code of practice; and which is misrepresented on that certificate or in a repository

the liability of HKPost to any Subscriber and any Relying Party, whether as Subscriber or Relying Party as defined by the CPS or in any other capacity at all, is limited to, and shall not under any circumstances exceed, HK$200,000 per certificate (whether it be g-Cert (Individual) or g-Cert (Functional Unit)) irrespective of the number of claim(s), breach(es) and/or loss(es) mentioned above.

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

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

Any liability for 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.

If, there is any loss caused by reliance on a false or forged digital signature of a subscriber or any person purportedly acting on behalf of the subscriber supported by a certificate issued by the HKPost(or its Contractor acting on its behalf), if the HKPost has complied with the requirements of the Ordinance and the COP, the HKPost the Contractor and their respective officers, employees or agents, accept no responsibility for any loss or damage to the Subscriber and the Relying Parties and any Reliance Limit that applies to any certificate in these circumstances is not necessary due to the aforementioned disclaimer.

9.9 Indemnities

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

"The Postmaster General acting by the officers of the Hong Kong Post Office and the Contractor has issued this certificate as a Recognized CA under the Electronic Transactions Ordinance (Cap. 553) upon the terms and conditions set out in the Postmaster General's Certification Practice Statement (CPS) that applies to this certificate.

Accordingly, any person, before relying upon this certificate should read the CPS that applies to g-Certs which may be read on the HKPost CA web site at www.eCert.gov.hk. The laws of Hong Kong SAR apply to this certificate and Relying Parties must submit any dispute or issue arising as a result of their reliance upon this certificate to the non-exclusive jurisdiction of the Courts of Hong Kong SAR.

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

The Postmaster General (by the Hong Kong Post Office, the Contractor and their respective officers, employees and agents) issues this certificate without undertaking any responsibility or duty of care to Relying Parties save as set out in the CPS.

Relying Parties, before relying upon this certificate are responsible for:

a. *Relying on it only when reliance is reasonable and in good faith in the light of all the circumstances known to the Relying Party at the time of reliance;*
b. *Before relying upon this certificate, determining that the use of the certificate and any digital signature supported by it is appropriate for its purposes under the CPS;*
c. *Checking the status of this certificate on the Certificate Revocation List whenever applicable, prior to reliance; and*
d. *Performing all appropriate certificate path validation procedures.*

If, there is any loss caused by reliance on a false or forged digital signature of a subscriber supported by a certificate issued by the Postmaster General, Hong Kong Post Office, (or its Contractor acting on its behalf), if the Postmaster General has complied with the requirements of the Ordinance and the code of practice with respect to that certificate , the Postmaster General, the Contractor and their respective officers, employees or agents, accept no responsibility for any loss or damage to the Relying Parties and any Reliance Limit that applies to this certificate under the Ordinance in these circumstances is not necessary due to the aforementioned disclaimer.

Subject to the requirements and exceptions specified in the CPS including Sections 9.8 and 9.9 of the CPS and those as stated in this certificate, in the event of HKPost's breach of any duty of care, and in particular, under the CPS or in law to exercise reasonable skill and care and/or any duties that may be owed to a Relying Party because any certificate issued by HKPost under the public key infrastructure initiative is relied upon or used by a Relying Party or any one else whomsoever, or a loss caused by reliance

on any information that HKPost is required to confirm according to this CPS and the code of practice; and which is misrepresented on that certificate or in a repository
the liability of HKPost to any Relying Party or any one else whomsoever, is limited to, and shall not under any circumstances exceed, HK$200,000 per certificate (whether it be g-Cert (Individual) or g-Cert (Functional Unit)) irrespective of the number of claim(s), breach(es) and/or loss(es) mentioned above.

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

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

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

9.10 Term and Termination

9.10.1 Term
The CPS changes will be effective upon publication by HKPost in the HKPost CA website at http://www.eCert.gov.hk or in the HKPost Repository and are binding on all current and subsequent Applicants and Subscribers to whom certificates are issued.

HKPost shall notify the Commissioner for Digital Policy any subsequent changes to this CPS as soon as practicable.

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

9.10.3 Effect of Termination and Survival
In the event that HKPost ceases to operate as a CA, notification to the 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 shall properly archive the CA Records including certificates issued, root certificates, Certification Practice Statements and Certificate Revocation Lists for 7 years after the date of service termination.

9.11 Individual Notices and Communications with Participants

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

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

Hongkong Post Certification Authority

Kowloon East Post Office Box 68777

Email: enquiry@eCert.gov.hk

9.12 Amendments

9.12.1 Procedure for Amendment

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

Subscriber Agreement cannot be varied, amended or changed except to comply with a variation or change in this CPS or with the express written consent of the Postmaster General. In the event of a conflict between this CPS and the Subscriber Agreement, other rules, guidelines, or contracts, the Subscriber, Relying Parties and HKPost shall be bound by the provisions of this CPS, except to the extent that the provisions are prohibited by law.

9.12.2 Notification Mechanism and Period

HKPost shall notify the 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.

9.12.3 Circumstances Under Which OID Must be Changed

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

9.13 Dispute Resolution Provisions

Subject to Section 9.15 below, the decisions of HKPost pertaining to matters within the scope of this CPS are final in the absence of any manifest error. Any claims that there has been manifest error should be submitted to HKPost at the following address:

Hongkong Post Certification Authority

Kowloon East Post Office Box 68777

Email: enquiry@eCert.gov.hk

9.14 Governing Law

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

9.15 Compliance with applicable law

9.15.1 Jurisdiction

A party whether HKPost or a Subscriber or a Relying Party or the Contractor or RA (each a Party) shall first refer any dispute or difference arising out of or in connection with this CPS to mediation in accordance with The Government of the Hong Kong Special Administrative Region Mediation Rules prevailing at the time.

If the said dispute or difference is not settled by mediation according to above, a Party may institute litigation in respect of the said dispute or difference. The Parties agree that the courts of Hong Kong shall have exclusive jurisdiction in respect of the said dispute or difference.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

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

9.16.2 Assignment

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

9.16.3 Severability

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

9.16.4 Enforcement (Non-Waiver of Rights)

Hongkong Post's failure to enforce a provision of this CPS does not waive Hongkong Post's right to enforce the same provisions later or right to enforce any other provisions of this CPS. To be effective any waivers must be in writing and signed by Hongkong Post.

9.16.5 Force Majeure

HKPOST INCURS NO LIABILITY IF IT IS PREVENTED, FORBIDDEN OR DELAYED FROM PERFORMING, OR OMITS TO PERFORM, ANY ACT OR REQUIREMENT BY REASON OF: ANY PROVISION OF ANY APPLICABLE LAW, REGULATION OR ORDER; CIVIL, GOVERNMENTAL OR MILITARY AUTHORITY; THE FAILURE OF ANY ELECTRICAL, COMMUNICATION OR OTHER SYSTEM OPERATED BY ANY OTHER PARTY OVER WHICH IT HAS NO CONTROL; FIRE, FLOOD, OR OTHER EMERGENCY CONDITION; STRIKE; ACTS OF TERRORISM OR WAR; ACT OF GOD; OR OTHER

SIMILAR CAUSES BEYOND ITS REASONABLE CONTROL AND WITHOUT ITS FAULT OR NEGLIGENCE.

9.17 Other Provisions

9.17.1 No Supply of Goods

For the avoidance of doubt, a Subscriber Agreement is not a contract for the supply of goods of any description or at all. Any and all certificates issued pursuant to it remain the property of and in the possession and control of HKPost and no right, title or interest in the certificates is transferred to the Subscriber, who merely has the right to procure the issue of a certificate and to rely upon it and the certificates of other Subscribers in accordance with the terms of the Subscriber Agreements. Accordingly the Subscriber Agreements contain (or are to contain) no express or implied terms or warranties as to the merchantability or fitness of a certificate for a particular purpose or any other terms or conditions appropriate in a contract for the supply of goods. Equally HKPost, in making available the certificates in a public Repository accessible by Relying Parties is not supplying any goods to Relying Parties and likewise gives to Relying Parties no warranty as to the merchantability or fitness for a particular purpose of a certificate nor makes any other representation or warranty as if it were supplying goods to Relying Parties. HKPost agrees to transfer those articles into possession of Applicants or Subscribers for the limited purposes set out in this CPS. Nonetheless HKPost shall exercise reasonable care to see that the same is fit for the purposes of completing and accepting a certificate as set out in this CPS, and if it is not, then HKPost's liability shall be as set out in Section 9.8. In addition, the articles transferred from HKPost may contain other material not relevant to the completion and acceptance of an g-Cert, if it does, the legal position in relation to such material is not governed by the CPS or the Subscriber Agreement, but by separate terms and conditions that will be referred to in the terms and conditions enclosed in the articles.

Appendix A - Glossary and Acronyms

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

"Accept", in relation to a certificate

(a) in the case of a person named or identified in the certificate as the person to whom the certificate is issued, means to

  (i) confirm the accuracy of the information on the person as contained in the certificate;
  (ii) authorise the publication of the certificate to any other person or in a repository;
  (iii) use the certificate; or
  (iv) otherwise demonstrate the approval of the certificate; or

(b) in the case of a person to be named or identified in the certificate as the person to whom the certificate is issued, means to

  (i) confirm the accuracy of the information on the person that is to be contained in the certificate;
  (ii) authorise the publication of the certificate to any other person or in a repository; or
  (iii) otherwise demonstrate the approval of the certificate.

"Applicant" means a subscriber organisations listed in Appendix E acting through the Requestor.

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

"Application Interface" or **"API"** means an application programming interface which defines the interaction between CMMP system and specific B/D/O system. CMMP receives user account information from specific B/D/O system via the API when B/D/O manages their user accounts in their system.

"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.

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

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

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

"Business Administrator" means a user role in CMMP responsible for verifying the identity of the Applicant (i.e. acting as a Registration Authority) and approving the requests of certificate application, renewal and revocation in the CMMP.

"CA" means Certification Authority.

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

"Certificate" or "g-Cert" means a Record which:-

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

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

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

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

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

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

"CMMP" means the centrally managed service platform under the administration and support of DPO as listed in **Appendix E**, which provides the functions summarised in Section 9.6.5.1 above.

"CMMP User" means the B/D/Os users who are provided with an account by DPO to login the CMMP to access various Designated Applications.

"Compromised Key Reporting web page" is a web page in HKPost CA website for reporting of suspected Private Key Compromise related to certificates.

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

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

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

"CPS" means Certification Practice Statement.

"Designated Application" means, the Designated Applications set out in **Appendix H**.

"Digital Signature", in relation to an Electronic Record, means an Electronic Signature of the signer generated by the transformation of the Electronic Record using an Asymmetric Cryptosystem and a hash function such that a person having the initial untransformed Electronic Record and the signer's Public Key can determine:

(a) whether the transformation was generated using the Private Key that corresponds to the signer's Public Key; and
(b) whether the initial Electronic Record has been altered since the transformation was generated.

"Domain Name" means a label assigned to a node in the Domain Name System.

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

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

"**DPO**" means the Digital Policy Office of the Government.

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

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

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

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

"g-Cert (Individual)" or "g-Cert (Functional Unit)" may each be referred to as g-Cert or certificate.

"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.

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

"Hong Kong" means the Hong Kong Special Administrative Region of the People's Republic of China.

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

"Information System" means a system which -

(a) processes Information;
(b) records Information;
(c) can be used to cause Information to be recorded, stored or otherwise processed in other Information systems (wherever situated); and
(d) can be used to retrieve Information, whether the Information is recorded or stored in the system itself or in other Information systems (wherever situated).

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

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

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

"Key Pair", in an Asymmetric Cryptosystem, key pair means a Private Key and its mathematically related Public Key, where the Public Key can verify a Digital Signature that the Private Key generates.

"Mailbox Field", in g-Cert, it means contains a Mailbox Address of the Subject via rfc822Name or otherName value of type id-on-SmtpUTF8Mailbox in the subjectAltName extension.

"OCSP" means Online Certificate Status Protocol.

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

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

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

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

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

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

"RA" means Registration Authority.

"Recognized CA" means Recognized Certification Authority.

"Recognized Certificate" means

(a) a certificate recognized under Section 22 of Electronic Transactions Ordinance;
(b) a certificate of a type, class or description of certificate recognized under Section 22 of Electronic Transactions Ordinance; or

(c) a certificate designated as a recognized certificate issued by the Certification Authority referred to in Section 34 of Electronic Transactions Ordinance.

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

"Reliable Method of Communication" means a method of communication, such as a postal/courier delivery address, telephone number, or email address.

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

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

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

"Relying Party" means a CMMP user or functional unit of a Subscriber Organisation through the use of CMMP to verify the identity of another CMMP user or functional unit before trusting a digitally signed message from such CMMP user or functional unit.

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

"Requester" means a user role in CMMP to raise a request of certificate application, certificate renewal and certificate revocation for the Subscriber Organisation.

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

"Role" means the function or the responsibility of the CMMP 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.

"S/MIME" is the acronym of Secure/Multipurpose Internet Mail Extension(s), being the standard and related certificate usage framework for securing electronic mail messages, including message signing and encryption. When referenced in a certificate's Extended Key Usage extension, it denotes the specific object identifier(s) and key purpose identifier(s) required or permitted by the latest applicable S/MIME BR, relevant RFCs, and the applicable certificate profile.

"SSL" is the acronym of Secure Sockets Layer.

"Sub CA" means the subordinate Certification Authority certificate which is issued by the Root CA "Hongkong Post Root CA 2" and is used to Sign the Hongkong Post Recognized Certificates.

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

"Subscriber" means a Subscriber Organisation

"Subscriber Agreement" means an agreement between HKPost (viz the Postmaster General) representing the Government and the Subscriber which comprises the which comprises the Subscriber Terms and Conditions of g-Cert Certificates and this CPS. It is a memorandum of understanding and is not legally binding.

"Subscriber Organisation" means an entity listed in Appendix E.

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

"TLS" is the acronym of Transport Layer Security.

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

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

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

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 g-Cert Format

This appendix provides the formats of g-Cert (Individual) and g-Cert (Functional Unit) issued by the Sub CA "Hongkong Post g-Cert CA 2 - 26" under this CPS.

1) g-Cert (Individual) Certificate Format

Field Name		Field Content
Standard fields		
Version		X.509 v3
Serial number		[20-byte hexadecimal number randomly generated by HKPost CA system]
Signature algorithm ID		sha256RSA
Issuer name		cn=Hongkong Post e-Cert CA 2 - 26, 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=[CMMP User's name] (Note 1) g=[CMMP User's given name] sn=[CMMP User's surname] e=[email address] (Note 2) ou=[Subscriber Organisation branch/dept] o=Hong Kong SAR Government c=HK Object Identifier (2.5.4.5) SERIALNUMBER=[SRN] (Note 3) Object Identifier (OID: 2.5.4.97)=GOVHK
Subject public key info		Algorithm ID: RSA Public Key: 2048-bit key size
Issuer unique identifier		Not used
Subject unique identifier		Not used
Standard extension (Note 5)		
Authority Information Access	**Certification Authority Issuer**	URL=http://www1.eCert.gov.hk/root/ecert_ca_2-26.crt
Authority Key Identifier	**KeyID**	[Subject Key Identifier of the issuer's certificate]
Subject Key Identifier		[Derived from the Subject's public key]
Key usage		Non-repudiation, Digital Signature, Key Encipherment **(This field will be set Critical.)**
Certificate policies (Note 4)		Policy Identifier = [OID of this CPS] (Note 6) Policy Identifier = 2.23.140.1.5.3.3 (Note 7) Policy Identifier = 1.3.6.1.4.1.16030.1.10.4 (Note 8)
Subject alternative name	**rfc822**	[email address] (Note 2)
Issuer alternative name		Not used
Basic constraints	**Subject type**	Not used
	Path length constraint	Not used
Extended key usage		S/MIME
CRL distribution points		Distribution Point Name = [URL of CRL Distribution Point] (Note 9)

Note
1. CMMP User's name format: Surname (in capital) + Given name (e.g. CHAN Tai Man David).
2. Email address of the CMMP User provided by Subscriber Organisation.
3. SRN: 10-digit Subscriber Reference Number.
4. The certificate issued under this Sub CA is in compliance with this CPS, Baseline Requirements for S/MIME published by CA/Browser Forum.

5. All standard extensions are set as “non-critical” unless otherwise specified.
6. The OID of this CPS is included in this field. Please refer to Section 1.2 of this CPS for the OID of this CPS.
7. Policy object ID assigned by the CA / Browser Forum, for certificates complying with Sponsor-validated Strict Certificate Policy.
8. This HKPCA-assigned OID indicates that the holder is a g-Cert (Individual) subscriber.
9. URL of CRL Distribution Point is http://crl1.eCert.gov.hk/crl/eCertCA2-26CRL1.crl which is a full CRL issued by the Sub CA “Hongkong Post e-Cert CA 2 - 26”.

2) g-Cert (Functional Unit) Certificate Format

Field Name		Field Content
Standard fields		
Version		X.509 v3
Serial number		[20-byte hexadecimal number randomly generated by HKPost CA system]
Signature algorithm ID		sha256RSA
Issuer name		cn=Hongkong Post e-Cert CA 2 - 26, 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=Hong Kong SAR Government e=[email address] (Note 1) ou=[Name of Bureau/Depart/Office] o=Hong Kong SAR Government c=HK Object Identifier (2.5.4.5) SERIALNUMBER=[SRN] (Note 2) Object Identifier (OID: 2.5.4.97)=GOVHK
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 4)		
Authority Information Access	**Certification Authority Issuer**	URL=http://www1.eCert.gov.hk/root/ecert_ca_2-26.crt
Authority Key Identifier	**KeyID**	[Subject Key Identifier of the issuer's certificate]
Subject Key Identifier		[Derived from the Subject's public key]
Key usage		Digital Signature, Key Encipherment **(This field will be set Critical.)**
Certificate policies (Note 3)		Policy Identifier = [OID of this CPS] (Note 5) Policy Identifier = 2.23.140.1.5.2.3 (Note 6) Policy Identifier = 1.3.6.1.4.1.16030.1.10.5 (Note 7)
Subject alternative name	**rfc822**	[email address](Note 1)
Issuer alternative name		Not used
Basic constraints	**Subject type**	Not used
	Path length constraint	Not used
Extended key usage		S/MIME
CRL distribution points		Distribution Point Name = [URL of CRL Distribution Point] (Note 8)

Note
1. Email address of the CMMP Function Unit provided by Subscriber Organisation.
2. SRN: 10-digit Subscriber Reference Number.
3. The certificate issued under this Sub CA is in compliance with this CPS, Baseline Requirements for S/MIME published by CA/Browser Forum.
4. All standard extensions are set as “non-critical” unless otherwise specified.
5. The OID of this CPS is included in this field. Please refer to Section 1.2 of this CPS for the OID of this CPS.
6. Policy object ID assigned by the CA / Browser Forum, for certificates complying with Organisation-validated Strict Certificate Policy.
7. This HKPCA-assigned OID indicates that the holder is a g-Cert (Functional Unit) subscriber.
8. URL of CRL Distribution Point is http://crl1.eCert.gov.hk/crl/eCertCA2-26CRL1.crl which is a full CRL issued by the Sub CA “Hongkong Post e-Cert CA 2 - 26”.

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 as well as the format of the Certificate Revocation Lists (CRLs) that are issued by the Sub CA "Hongkong Post e-Cert CA 2 - 26" and the Authority Revocation Lists (ARLs) that are issued by the root CA "Hongkong Post Root CA 2".

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

a) **Full CRL** that contains Information of all revoked certificates that are issued by the Sub CA "Hongkong Post e-Cert CA 2 - 26". The Full CRL for g-Cert is available for public access at :-

http://crl1.eCert.gov.hk/crl/eCertCA2-26CRL1.crl; or
ldap://ldap1.eCert.gov.hk (port 389, cn=Hongkong Post e-Cert CA 2 - 26 CRL1, o=Hongkong Post, c=HK)

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

Under normal circumstances, HKPost 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 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 Full CRL issued by the Sub CA "Hongkong Post e-Cert CA 2 - 26" under this CPS:

Standard Fields	Sub-fields	Field Contents of Full CRL	Remarks
Version		v2	This field describes the version of encoded CRL as X.509 v2.
Signature algorithm ID		sha256RSA	This field contains the algorithm identifier for the algorithm used to sign the CRL.
Issuer name		cn=Hongkong Post e-Cert CA 2 - 26, o=Hongkong Post, l=Hong Kong, s=Hong Kong, c=HK	This field identifies the entity who has signed and issued the CRL.
This update		[UTC time]	"This Update" indicates the date the CRL was generated.

Standard Fields	Sub-fields	Field Contents of Full CRL	Remarks
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 3)			
Authority Key Identifier	**KeyID**	[Subject Key Identifier of the Sub CA issuing this CRL]	
CRL number		[Generated by CA system]	The CRL Number is generated in sequence for each CRL issued by a CA.

(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.
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 2)
Standard extension (Note 3)			

Standard Fields	Sub-fields	Field Contents of ARL	Remarks
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 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. For CRL relating to g-Cert, the following reason codes may be included in the field:

   1 = keyCompromise, 3 = affiliationChanged, 4 = superseded,
   5 = cessationOfOperation, 9 = privilegeWithdrawn

   Otherwise, no revocation reason code will be included.

2. For ARL relating to Root CA or Sub CA Certificates, one of the following reason codes must be included in the field:

   1 = keyCompromise , 2 = cACompromise, 3 = affiliationChanged ,
   4 = superseded, 5 = cessationOfOperation

3. All fields will be set “non-critical” unless otherwise specified.

Appendix D - Summary of Hongkong Post g-Cert Features

Features (Note 1)	**g-Cert Certificate**
Subscriber Organisation	Bureaux/Departments/Offices of the Government of Hong Kong SAR
Subscriber	CMMP User / CMMP functional unit
Reliance Limit	HK$200,000
Recognized Certificate	Yes
Key pair size	2048-bit RSA
Registration Authority	Business Administrator of CMMP system at respective B/D/Os
Key pair generation	Key generation by CMMP
Identity verification	As mentioned in Section 3.2
Usage of certificate	•Encryption / Decryption, and generation of signature for acknowledge receipt of message. •Sign document and perform authentication within CMMP (not to serve as digital signature under ETO) (for g-Cert (Individual) only) •Used in the Designated Applications of the corresponding g-Cert as specified in **Appendix H**
Subscriber's information included in the certificate	▪ Subscriber Organisation's name ▪ CMMP User's name and email address (for g-Cert (Individual)); ▪ Functional Unit's email address (for g-Cert (Functional Unit)) ▪ Subscriber Reference Number (SRN) generated by the HKPost system
Subscription fees and certificate validity	Certificate validity is one year. See **Appendix H**

Note

1. Prior arrangement between the subscriber organisation and HKPost is required before HKPost will issue g-Cert certificates for that subscriber.

Appendix E - List of Subscriber Organisation / Registration Authorities and CMMP for the Hongkong Post g-Cert, if any

(I) List of B/D/O as Subscriber Organisation / Registration Authority for HKPost

Name of B/D/O as Subscriber Organisation / Registration Authority for HKPost	Classes of Certificate(s)	Services to be Provided
Agriculture, Fisheries and Conservation Department Architectural Services Department Audit Commission Auxiliary Medical Service Buildings Department Census and Statistics Department Chief Executive's Office Chief Executive's Policy Unit Chief Secretary for Administration's Office – Government Records Service Chief Secretary for Administration's Office and Financial Secretary's Office Civil Aid Service Civil Aviation Department Civil Engineering and Development Department Civil Service Bureau	g-Cert (Individual) and g-Cert (Functional Unit)	The following processes of g-Cert applications for CMMP:- - certificate applications as set out in Sections 3.2 and 4.1. - certificate renewal request as set out in Section 4.6. - certificate revocation request as set out in Section 4.9.1, 4.9.3 and 4.9.5. - protection of documents by B/D/O as set out in Section 5.1.6.

Name of B/D/O as Subscriber Organisation / Registration Authority for HKPost	Classes of Certificate(s)	Services to be Provided
Commerce and Economic Development Bureau		
Companies Registry		
Constitutional and Mainland Affairs Bureau		
Correctional Services Department		
Cultural and Creative Industries Development Agency		
Culture, Sports and Tourism Bureau		
Customs and Excise Department		
Department of Health		
Department of Justice		
Development Bureau – Planning and Lands Branch		
Development Bureau – Works Branch		
Drainage Services Department		
Education Bureau		
Electrical and Mechanical Services Department		
Environment and Ecology Bureau		
Environmental Protection Department		
Financial Services and the Treasury Bureau – Financial Services Branch		
Financial Services and the Treasury Bureau – The Treasury Branch		
Fire Services Department		

Name of B/D/O as Subscriber Organisation / Registration Authority for HKPost	Classes of Certificate(s)	Services to be Provided
Food and Environmental Hygiene Department		
Government Flying Service		
Government Laboratory		
Government Logistics Department		
Government Property Agency		
Health Bureau		
Highways Department		
Home Affairs Department		
Home and Youth Affairs Bureau		
Hong Kong Monetary Authority		
Hong Kong Observatory		
Hong Kong Police Force		
Housing Bureau		
Housing Department		
Immigration Department		
Independent Commission Against Corruption		
Independent Police Complaints Council		
Information Services Department		

Name of B/D/O as Subscriber Organisation / Registration Authority for HKPost	Classes of Certificate(s)	Services to be Provided
Inland Revenue Department Innovation, Technology and Industry Bureau Innovation, Technology and Industry Bureau – Digital Policy Office Innovation, Technology and Industry Bureau – Innovation and Technology Commission Intellectual Property Department Invest Hong Kong Joint Secretariat for the Advisory Bodies on Civil Service and Judicial Salaries and Conditions of Service Judiciary Labour and Welfare Bureau Labour Department Land Registry Lands Department Legal Aid Department Leisure and Cultural Services Department Marine Department Office of the Communications Authority Office of the Ombudsman Official Receiver's Office		

Name of B/D/O as Subscriber Organisation / Registration Authority for HKPost	Classes of Certificate(s)	Services to be Provided
Planning Department Post Office Public Service Commission Radio Television Hong Kong Rating and Valuation Department Registration and Electoral Office Secretariat, Commissioner on Interception of Communications and Surveillance Security Bureau Social Welfare Department The Hong Kong Economic and Trade Offices Trade and Industry Department Transport and Logistics Bureau Transport Department Treasury University Grants Committee Secretariat Water Supplies Department Working Family and Student Financial Assistance Agency (Student Finance Office) Working Family and Student Financial Assistance Agency (Working Family Allowance Office)		

(II) CMMP

CMMP Administration and Support	Classes of Certificate(s)	Services to be Provided	Remarks
Digital Policy Office	Hongkong Post g-Cert (Individual) and g-Cert (Functional Unit)	Setup and Maintenance the CMMP System for B/D/O: - with user roles for B/D/O to perform functions related to g-Cert applications; - provide approval workflow for the process off certificate application, renewal and revocation; - provide safe custody of g-Cert subscribers' Private Key and its use; - upon request by B/D/O, provide the g-Cert subscriber's Private Key to B/D/Os The following processes of g-Cert applications for B/D/O applicants:- - Define user role in CMMP to allow B/D/O to assign staff to act as Registration Authority for verifying the identity of Applicant as set out in Section 3.2. - key generation as set out in Sections 3.2.1, 4.3 and 4.6. - take responsibilities of the obligations as set out in Section 9.6.5.2.	For segregation of duties, the CMMP should not allow a user who acts as "Business Administrator" role to approve a request that is raised by oneself, that is for a request, a CMMP User cannot be acting both the "Business Administrator" and the "Requester".

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

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

Appendix G - Lifespan of CA root certificates

Reference	Name of the HKPost CA root certificate	Lifespan	Remarks
1	Hongkong Post Root CA 2	5 September 2015 - 5 September 2040	This root CA commences to issue Sub CAs with effect from 5 September 2015.
Subject DN C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post Root CA 2 SHA-1 Thumbprint DE010808E41EC41930D44095F8FE596B582C8CA2			
2	Hongkong Post e-Cert CA 2 - 26	7 May 2026 - 5 September 2040	This Sub CA issues g-Cert from 1 October 2026.
Subject DN C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post e-Cert CA 2 - 26 SHA-1 Thumbprint EA9AECB58CB9023AE090235EA2FFFA8ED8420A88			

Appendix H - List of the Designated Applications of Hongkong Post g-Cert Certificates

g-Cert Type	Certificate Validity	Designated Application	Subscription Fees	Remarks
g-Cert (Individual)	1 year	DPO applications supported by CMMP	New application or renewal: HK$20 per certificate per year Promotional discount on subscription fees for g-Cert (Individual) certificates is offered by the Contractor. For details on the promotional discount, please refer to HKPost web site at http://www.ecert.gov.hk or make enquiry to Hongkong Post Certification Authority through the means provided in Section 1.5.2.	Use of g-Cert (Individual) for the purpose as set out in Section 1.3.4.1.1.
g-Cert (Functional Unit)	1 year	DPO applications supported by CMMP	New application or renewal: HK$20 per certificate per year	Use of g-Cert (Functional Unit) for the purpose as set out in Section 1.3.4.1.2.