THE CERTIFICATION PRACTICE STATEMENT

OF

THE HONG KONG INTERNET REGISTRATION CORPORATION LIMITED

As

A Recognized Certification Authority
under the Electronic Transactions Ordinance

for

HKCA d-Cert (Server)

Date : [TBC]
OID : 1.3.6.1.4.1.64092.1.7.1

Table of Contents

PREAMBLE 8
1. INTRODUCTION 10
1.1 Overview 10
1.2 Document Name and Identification 11
1.3 PKI Participants 11
1.3.1 Certification Authorities 11
1.3.2 Registration Authorities 11
1.3.3 Subscribers 12
1.3.3.1 Classes of Subscribers 12
1.3.4 Relying Parties 13
1.3.5 Other participants 13
1.4 Certificate Usage 13
1.4.1 Appropriate Certificate Uses 13
1.4.2 Prohibited Certificate Uses 13
1.5 Policy Administration 13
1.5.1 Organisation Administering the Document 13
1.5.2 Contact Person 14
1.5.3 Person Determining CPS Suitability for the Policy 14
1.5.4 CPS Approval Procedures 14
1.6 Definition and Acronyms 14
2. Publication and Repository Responsibilities 14
2.1 Repositories 14
2.2 Publication of Certification Information 14
2.3 Time or Frequency of Publication 14
2.4 Access Controls on Repositories 15
3. Identification and Authentication 16
3.1 Naming 16
3.1.1 Type of Names 16
3.1.2 Need for Names to be Meaningful 16
3.1.3 Anonymity or Pseudonymity of Subscribers 16
3.1.4 Rules for Interpreting Various Name Forms 17
3.1.5 Uniqueness of Names 17
3.1.6 Recognition, Authentication, and Role of Trademarks 17
3.2 Initial Identity Validation 17
3.2.1 Method to Prove Possession of Private Key 17
3.2.2 Authentication of Organisation Identity 18
3.2.3 Authentication of Individual Identity 20
3.2.4 Non-Verified Subscriber Information 20
3.2.5 Validation of Authority 20
3.2.6 Criteria for Interoperation 20
3.2.7 Authentication of Domain Names 21
3.2.8 Authentication of IP Addresses 21
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 Request 21
4. Certificate Life-Cycle Operational Requirements 21
4.1 Certificate Application 21
4.1.1 Who Can Submit a Certificate Application 21
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
4.3.1 CA Actions during Certificate Issuance 23
4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate 23
4.4 Certificate Acceptance 24
4.4.1 Conduct Constituting Certificate Acceptance 24
4.4.2 Publication of the Certificate by the CA 24
4.4.3 Notification of Certificate Issuance by the CA to Other Entities 24
4.5 Key Pair and Certificate Usage 24
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 25
4.6.1 Circumstances for Certificate Renewal 25
4.6.2 Who May Request Renewal 25
4.6.3 Processing Certificate Renewal Requests 25
4.6.4 Notification of New Certificate Issuance to Subscriber 26
4.6.5 Conduct Constituting Acceptance of a Renewal Certificate 26
4.6.6 Publication of the Renewal Certificate by the CA 26
4.6.7 Notification of Certificate Issuance by the CA to Other Entities 26
4.7 Certificate Re-Key 26
4.7.1 Circumstances for Certificate Re-Key 26
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 27
4.8.2 Who May Request Certificate Modification 27
4.8.3 Processing Certificate Modification Requests 27
4.8.4 Notification of New Certificate Issuance to Subscriber 27
4.8.5 Conduct Constituting Acceptance of Modified Certificate 27
4.8.6 Publication of the Modified Certificate by the CA 27
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 29
4.9.3 Procedure for Revocation Request 29
4.9.4 Revocation Request Grace Period 30
4.9.5 Time within Which CA Must Process the Revocation Request 30
4.9.6 Revocation Checking Requirements for Relying Parties 31
4.9.7 CRL Issuance Frequency 31
4.9.8 Maximum Latency for CRLs 31
4.9.9 On-Line Revocation/Status Checking Availability 31
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 32
4.9.14 Who Can Request Suspension 32
4.9.15 Procedure for Suspension Request 32
4.9.16 Limits on Suspension Period 32
4.10 Certificate Status Services 32

4.10.1 Operational Characteristics 32
4.10.2 Service Availability 32
4.10.3 Operational Features 32
4.11 End of Subscription 32
4.12 Key Escrow and Recovery 33
4.12.1 Key Escrow and Recovery Policy and Practices 33
4.12.2 Session Key Encapsulation and Recovery Policy and Practices 33
5. Facility, Management, and Operational Controls 34
5.1 Physical Controls 34
5.1.1 Site Location and Construction 34
5.1.2 Physical Access 34
5.1.3 Power and Air Conditioning 34
5.1.4 Water Exposures 34
5.1.5 Fire Prevention and Protection 34
5.1.6 Media Storage 34
5.1.7 Waste Disposal 34
5.1.8 Off-site Backup 35
5.2 Procedural Controls 35
5.2.1 Trusted Roles 35
5.2.2 Number of Personnel Needed for Each Task 35
5.2.3 Identification and Authentication of Each Role 35
5.2.4 Roles requiring Segregation of Duties 35
5.3 Personnel Controls 35
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 36
5.3.5 Job Rotation Frequency and Sequence 36
5.3.6 Sanctions for Unauthorised Actions 36
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 38
5.5 Records Archival 38
5.5.1 Types of Records Archived 38
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 39
5.7.1 Incident and Compromise Handling Procedures 39
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 40

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) 42
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 42
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 43
6.5 Computer Security Controls 43
6.5.1 Specific Computer Security Technical Requirements 43
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 44
6.7 Network Security Controls 44
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) 49
7.2.2 CRL and CRL Entry Extensions 49
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
9.2 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 52
9.3.1 Scope of Confidential Information 52
9.3.2 Information Not Within the Scope of Confidential Information 52
9.3.3 Responsibility to Protect Confidential Information 52
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 53
9.4.6 Disclosure Pursuant to Judicial or Administrative Process 53
9.4.7 Other Information Disclosure Circumstances 53
9.5 Intellectual Property rights 53
9.6 Representations and Warranties 54
9.6.1 CA Representations and Warranties 54
9.6.2 RA Representations and Warranties 54
9.6.3 Subscriber Representations and Warranties 54
9.6.4 Relying Party Representations and Warranties 55
9.6.5 Representations and Warranties of Other Participants 56
9.7 Disclaimers of Warranties 56
9.8 Limitations of Liability 57
9.9 Indemnities 58
9.10 Term and Termination 59
9.10.1 Term 59
9.10.2 Termination 59
9.10.3 Effect of Termination and Survival 59
9.11 Individual Notices and Communications with Participants 60
9.12 Amendments 60
9.12.1 Procedure for Amendment 60
9.12.2 Notification Mechanism and Period 60
9.12.3 Circumstances Under Which OID Must be Changed 60
9.13 Dispute Resolution Provisions 60
9.14 Governing Law 60
9.15 Compliance with Applicable Law 60
9.16 Miscellaneous Provisions 61
9.16.1 Entire Agreement 61
9.16.2 Assignment 61
9.16.3 Severability 61
9.16.4 Enforcement (Attorney's Fees and Waiver of Rights) 61

9.16.5 Force Majeure 61
9.17 Other Provisions 61
9.17.1 No Supply of Goods 61
Appendix A – Glossary and Acronyms 63
Appendix B - HKCA d-Cert Format 70
Appendix C - HKCA Certificate Revocation Lists (CRLs) and Authority Revocation List (ARL) 75
Appendix D - HKCA Online Certificate Status Protocol (OCSP) Response Format 79
Appendix E - Summary of HKCA d-Cert Certificates by Validation Type 81
Appendix F - List of Registration Authorities for the HKCA d-Cert, if any 82
Appendix G - List of Subcontractor(s) of Certizen Limited for HKCA d-Cert Services, if any 83
Appendix H - Lifespan of CA root certificates 84

PREAMBLE

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

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

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

Under the Ordinance, a Certification Authority may apply to the Commissioner for Digital Policy ("CDP") for recognition as a Recognized Certification Authority ("CA"). A Recognized CA may issue Certificates that are recognized by the CDP under section 22 of the Ordinance, as well as Certificates not recognized by the CDP. The Hong Kong Internet Registration Corporation Limited ("HKIRC") has decided so to pursue recognition as a Recognized CA.

Currently, HKIRC has awarded a contract ("Contract") to Certizen Limited for the operation and maintenance of the systems and services of the HKCA, as stipulated in this Certification Practice Statement ("CPS").

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

For the purposes of this document, the Hong Kong Internet Registration Corporation Limited is referred to as HKIRC or the Hong Kong Certification Authority (HKCA). It is expedient for HKCA to appoint Registration Authorities ("RAs") as its agents to carry out certain of the functions of HKCA as a Recognized CA as set out in this CPS. A list of Registration Authorities, if any, can be found in **Appendix F**.

HKCA remains a Recognized Certification Authority under Section 21 and 27 of the Ordinance and the Contractor and the RAs are agents of HKCA appointed pursuant to Section 3.2 of the Code of Practice for Recognized Certification Authorities ("Code of Practice") issued by the Commissioner for Digital Policy under Section 33 of the Ordinance. The Contractor and the RAs are capable of complying with the Code of Practice relevant to their operations as well.

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

HKCA, 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 online identification. The SSL/TLS certificates issued under this CPS (i.e. d-Cert (Server)) are Recognized Certificates under the Ordinance and are referred to as "certificates" or "d-Certs" in this CPS.

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

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

This CPS is designed to meet the latest version of the requirements of the following schemes:

- the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates ("Baseline Requirements") published by the CA / Browser Forum;
- Guidelines for the Issuance and Management of Extended Validation Certificates ("Extended Validation SSL certificate guidelines") published by the CA / Browser Forum;
- WebTrust Principles and Criteria for Certification Authorities;
- WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security;
- WebTrust Principles and Criteria for Certificate Authorities – Extended Validation SSL.

1. INTRODUCTION

1.1 Overview

This Certification Practice Statement ("CPS") is published for public knowledge by Hong Kong Internet Registration Corporation Limited ("HKIRC") and specifies the practices and standards that HKIRC, acting as the Hong Kong Certification Authority (HKCA), employs in issuing, revoking and publishing certificates.

HKCA 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.

The Internet Assigned Numbers Authority ("IANA") has assigned the Private Enterprise Number 64092 to HKIRC. For identification purpose, this CPS bears an Object Identifier ("**OID**") **"1.3.6.1.4.1.64092.1.7.1"** (see description of the field "Certificate Policies" in **Appendix B**). In addition to this OID, all certificates that comply with the Baseline Requirements will include the following additional identifiers:-

SSL certificates	Policy Object Identifier (OID)
Domain Validation d-Cert (Server) certificates	2.23.140.1.2.1 (assigned by the CA / Browser Forum, for certificates complying with Domain Validation (DV) policy)
Organisation Validation d-Cert (Server) certificates	2.23.140.1.2.2 (assigned by the CA / Browser Forum, for certificates complying with Organisation Validation (OV) policy)
Extended Validation d-Cert (Server) certificates	2.23.140.1.1 (assigned by the CA / Browser Forum, for certificates complying with Extended Validation (EV) policy)

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

Certificates issued by HKCA in accordance with this CPS will be relied upon by Relying Parties and used to verify Digital Signatures. Each Relying Party making use of a HKCA 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.

HKCA, as a Recognized CA, **has designated the d-Cert (Server) certificates issued under this CPS as Recognized Certificates.** This means for both Subscribers and Relying Parties, that HKCA has a legal obligation under the Ordinance to use a Trustworthy System for the issuance, revocation and publication in a publicly available Repository of accepted Recognized Certificates. Recognized Certificates have characteristics of accuracy and contain representations of fact which are defined in law by the Ordinance, including a representation

(as further defined below) that such certificates have been issued in accordance with this CPS. The fact that HKCA has appointed Registration Authorities as its agents does not diminish HKCA's obligation to use a Trustworthy System, nor does it alter the characteristics that d-Certs have as Recognized Certificates.

This CPS meets the format requirements of RFC 3647. While certain section titles are included in this CPS according to the structure of RFC 3647, the topic may not necessarily apply to services of HKCA. 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 HKCA's practices and procedures.

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

1.2 Document Name and Identification

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

Revision Number	Revision Description	Effective Date
1	Initial version of Certification Practice Statement for issuing d-Cert (Server).	[TBC]

1.3 PKI Participants

1.3.1 Certification Authorities

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

HKCA'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 HKCA 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.

HKCA, 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, HKCA 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 and provide OCSP responses in a timely manner (see Section 4.9); and
d) notify Subscribers of the revocation of their certificates (see Section 4.9.5).

1.3.2 Registration Authorities

Registration Authorities (RAs) are responsible only to HKCA under the terms of the agreement (the "RA Agreement") under which they are appointed by HKCA as its agents to carry out on HKCA's behalf certain of HKCA's obligations as detailed in this CPS. RAs, on behalf of HKCA,

collect and keep documents and information supplied under the terms of the CPS and Subscriber Agreements. HKCA 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 HKCA.

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

Refer to **Appendix F** - List of Registration Authorities for the HKCA d-Cert, if any.

1.3.3 Subscribers

Under this CPS, a Subscriber is the "Subscriber" or "Subscriber Organisation" referred to in **Appendix A**. For d-Certs that are issued via the RA or the Contractor as the agent of HKCA, the RAs and the Contractor do not owe a duty of care and are not responsible to the Relying Parties in any way for the issue of those d-Certs (see also Section 1.3.2). Subscribers who rely on a d-Cert of another Subscriber in a transaction will be Relying Parties in respect of such a certificate.

1.3.3.1 Classes of Subscribers

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

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

In accordance with the CA/B Forum-assigned Object Identifiers (OIDs), the d-Cert (Server) certificates are categorized into the following validation types.

i. Domain Validation d-Cert (Server) (DV d-Cert (Server)
   - Certificates are validated according to Domain Validation (DV) rules in compliance with the CA/Browser Forum Baseline Requirements.

ii. Organisation Validation d-Cert (Server) (OV d-Cert (Server)
   - Certificates are validated according to Organisation Validation (OV) rules in compliance with the CA/Browser Forum Baseline Requirements.

iii. Extended Validation d-Cert (Server) (EV d-Cert (Server)
   - Certificates are validated in accordance with the CA/Browser Forum Extended Validation (EV) guidelines.
   - EV d-Cert (Server) supports single or multiple server names only, but not server names with "Wildcard" character.

1.3.4 Relying Parties

Relying Parties are entities that have relied on any class or category of certificate issued by HKCA, including, but not limited to d-Cert for use in a transaction. For the avoidance of doubt, Relying Parties should not rely on the Registration Authorities.

1.3.5 Other participants

HKCA 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 HKCA to perform the services. In the event that such sub-contracting occurs, HKCA shall remain liable for the performance of the CPS and the Subscriber Agreement as if such sub-contracting had not occurred.

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

For details, refer to **Appendix G** - List of Subcontractor(s) of Certizen Limited for HKCA d-Cert Services.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

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

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

1.4.2 Prohibited Certificate Uses

Subscriber Organisations undertake to HKCA not to give authority to any person to use a digital signature of this class of certificate other than for the purpose of server authentication or establishment of secure communication channels with the server and accordingly any digital signature generated by the private key of this class of certificate used by a person other than for the aforesaid purposes must be treated as a signature generated and used without the authority of the subscriber organisation whose signature it is and must be treated for all purposes as an unauthorised signature.

1.5 Policy Administration

1.5.1 Organisation Administering the Document

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

1.5.2 Contact Person

Subscribers may send their enquiries, suggestions or complaints by:

Mail to : Unit 501, Level 5, Core C, Cyberport 3, 100 Cyberport Road, Hong Kong
Tel: (852) 31680680
Email: enquiry@hkca.hk

HKCA 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 HKCA 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

HKCA 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 HKCA. HKCA has the right to vary this CPS without notice (see Section 9.12).

1.6 Definition and Acronyms

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

2. Publication and Repository Responsibilities

2.1 Repositories

Under the Ordinance, HKCA maintains a Repository that contains a list of accepted certificates issued under this CPS, the current certificate revocation list, the current OCSP responses, the HKCA Public Key, a copy of this CPS, and other Information related to d-Cert (Server) certificates which reference this CPS, such as d-Cert application documents and the "Subscribers Terms and Conditions" enclosed in the application. This CPS and the latest version of "Subscribers Terms and Conditions" shall constitute the public Subscriber Agreement and Relying Party Agreement. HKCA shall promptly publish and update the Repository regarding the relevant disclosed documents and disclosure records of the previously published documents and their amendments.

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

2.2 Publication of Certification Information

The HKCA Repository can be accessed at URLs as follows:

https://www.hkca.hk
ldap://ldap.hkca.hk

2.3 Time or Frequency of Publication

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

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

2.4 Access Controls on Repositories

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

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

3. Identification and Authentication

3.1 Naming

3.1.1 Type of Names

3.1.1.1 Subject Name

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

a) The Subscriber Organisation's name as it is registered with the appropriate Hong Kong Government Department or Registration Agency or a Bureau/Department of the Government of the Hong Kong SAR or as a statutory body whose existence is recognized by the laws of Hong Kong SAR, or the official name of that Bureau or Department where the Subscriber Organisation is a Bureau or Department of the Government of Hong Kong SAR; and

b) The server name (including domain name of the server) owned by the Subscriber Organisation. There may be additional server name(s) in the Subject Alternative Name, and each additional server name must be owned by the Subscriber Organisation. No wildcard character (i.e. an asterisk character '*') will be allowed in any part of the additional server name(s).

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

3.1.1.2 The Authorised Representative

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

3.1.1.3 Organisation Names in Chinese Language

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

3.1.2 Need for Names to be Meaningful

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

3.1.3 Anonymity or Pseudonymity of Subscribers

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

3.1.4 Rules for Interpreting Various Name Forms

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

3.1.5 Uniqueness of Names

The Subject Name (referred to in **Appendix B**) shall be unambiguous and unique to a Subscriber. However, this CPS does not require that a specific component or element of a name be unique or unambiguous by itself. Domain name uniqueness is controlled by the Internet Corporation for Assigned Names and Numbers (ICANN).

3.1.6 Recognition, Authentication, and Role of Trademarks

Applicants and Subscribers warrant (promise) to HKCA and represent to Relying Parties that the Information supplied by them in the d-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 HKCA in matters concerning any disputes concerning the ownership of trademarks, service marks, domain name, trade name, company name, or any other intellectual property rights are discretionary and final.

3.2 Initial Identity Validation

All Applicants must submit their d-Cert applications either through the d-Cert Subscriber Portal, or through the Contractor or a RA, where applicable (see **Appendix E**).

Following approval of the application, HKCA prepares a d-Cert (Server) and notifies the Applicant of how the certificate may be issued as described in Section 4.3.

For d-Cert certificate applications submitted through the d-Cert Subscriber Portal, HKCA will verify, amongst other things, the following:

a) The Authorised Representative of the Organisation has created a corporate account on the d-Cert Subscriber Portal using "iAM Smart+" and has provided personal identity information consistent with their Hong Kong Identity Card (HKID).
b) The Authorised Representative has digitally signed the certificate application using "iAM Smart+", and the Organisation will be deemed the Subscriber.

HKCA will accept the authentication and digital signature of the Applicant provided through "iAM Smart+" as sufficient proof of identity.

For d-Cert certificate applications submitted through the Contractor or a RA, HKCA will verify the Applicant's personal details against the information provided by the Contractor or RA. HKCA reserves the absolute right to require the Applicant to furnish additional information or documentation, where HKCA considers it necessary, for the purpose of substantiating and verifying the applicant's personal identity in particular cases.

3.2.1 Method to Prove Possession of Private Key

The Applicant generates on his/her own devices the Certificate Signing Request (CSR) containing the public key, and transmits the CSR to HKCA through a designated web page at https://www.hkca.hk.

Upon receipt of the CSR, HKCA shall verify that the Applicant is in possession of the corresponding Private Key by checking the digital signature on the CSR structure containing the public key material. HKCA shall not have possession of the Applicant's Private Keys.

3.2.2 Authentication of Organisation Identity

Authentication of the identity of an Organisational Applicant is required for processing OV and EV d-Cert (Server) certificate applications and will be accomplished through one of the following processes:

a) The Applicant's Authorised Representative will submit the application through the d-Cert Subscriber Portal, and such application will be digitally signed by the Authorised Representative using "iAM Smart+".

b) At the sole discretion of HKCA, submission of the application package may be accepted without the Authorised Representative's personal attendance, provided that (1) the application is accompanied by a copy of the Authorised Representative's HKID Card or passport duly signed by the Authorised Representative, and (2) both of the following conditions are satisfied:
   i. the Authorised Representative's identity has been authenticated in a past application of the Subscriber Organisation, and the Authorised Representative has appeared at a HKCA's designated premise, or a premise of the Contractor or RA designated by HKCA for identity verification during such prior application; and
   ii. reasonable justification is available for re-affirming the identity of the Authorised Representative, which may include without limitation confirmation by means of a direct telephone call with the Authorised Representative or verification of the Authorised Representative's signature against records maintained from prior applications.

c) HKCA reserves the right, in its sole discretion, to reject any application where doubt arises as to the authenticity of the Authorised Representative's identity.

3.2.2.1 OV d-Cert (Server)

Each application for OV d-Cert (Server) certificates must be accompanied by the following documentation for verification by HKCA:

a) An authorisation letter bearing the "For and on behalf of" chop and the authorised signature(s) of the organisation by the Applicant giving authority to the Authorised Representative to make the application and prove the ownership of the domain name(s) to be identified in the Subject Name and Subject Alternative Name, if any, in the d-Cert (Server) certificate; and

b) Documentation issued by the appropriate Hong Kong Government Department or Registration Agency attesting the existence of the organisation. The validity of the documentation should not expire within one month by the time the application is submitted;

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

3.2.2.2 EV d-Cert (Server)

HKCA shall verify the authentication of the legal, physical, and operational existence of the organisation identity in relation to the Applicant in accordance with Section 11 of the CA / Browser Forum Extended Validation SSL certificate guidelines, as follows:

For a Government Entity or Private Organisation

a) For an organisation deemed as a Government Entity or a Private Organisation as defined in the CA / Browser Forum Extended Validation SSL certificate guidelines, each application for EV d-Cert (Server) certificates must be accompanied by the same documentation as stated in Section 3.2.2.1. For a Private Organisation that holds a valid business registration certificate issued by the Government of the Hong Kong SAR, HKCA shall verify the legal existence of the organisation with such documentation issued by the Registration Agency and the Incorporating Agency. For a Private Organisation that is a statutory body, HKCA shall verify the legal existence as recognized by the Laws of Hong Kong SAR and if necessary, further check any applicable documentation issued by the Incorporating Agency.

For a Business Entity

b) For an organisation deemed as a Business Entity as defined in the CA / Browser Forum Extended Validation SSL certificate guidelines, apart from the documentation issued by the Registration Agency as stated in Section 3.2.2.1, the Authorised Representative must also be accompanied by a Verified Professional Letter issued by a notary, a practising Certified Public Accountant (CPA) or a practising solicitor in Hong Kong ("Third-Party Validator"), which states that the following additional documentation ("Vetting Documents") have been verified by the Third-Party Validator:

   i) Personal Statement of the Applicant that includes full name or names by which a person is, or has been, known (including all other names used), residential address at which he/she can be located, date of birth, and an affirmation that all of the information contained in the certificate request is true and correct. The Personal Statement bears the Applicant's signature and that signature must be the same as that on application form;
   ii) Copy of the Applicant HKID card or passport; and
   iii) Copy of at least two documentary evidences to establish the Applicant's identity that include the name of the Applicant, one of which MUST be from a financial institution. (1) Acceptable financial institution documents includes a credit/debit card (provided that it contains an expiration date and it has not expired) or a mortgage statement/bank statement (that is less than six months old), and (2) acceptable non-financial documents include a recent original utility bill confirming the arrangement to pay for the services at a fixed address (not a mobile/cellular telephone bill) or a copy of a statement for payment of a lease (provided that the statement is dated within the past six months).
   iv) Copy of business registration certificate;
   v) Copy of Applicant organisation's active demand deposit account information with regulated financial institution

   All originals of the Vetting Documents above, must be submitted for verification by HKCA. HKCA shall conduct face-to-face validation with the Applicant and verify the originals of the Vetting Documents as follows:

   i) Attest to the content of the Personal Statement, to determine that the information including Applicant names, Applicant's signature and residential address is

consistently matched with the corresponding information in the originals of Vetting Documents and the application form; and

ii) Attest to the Vetting Documents, including copy of the Applicant's HKID card or passport that they are full, true, and accurate reproduction of the originals.

Upon receipt of Verified Professional Letter together with the attested Vetting Documents, HKCA shall verify whether the Third-Party Validator is a legally-qualified notary, a practising Certified Public Accountant (CPA) or a practising solicitor in Hong Kong and confirm whether the Third-Party Validator has verified the Vetting Documents properly.

For ALL OV and EV d-Cert (Server) applications:

c) When the address of place of business provided in the application form could not be verified with the appropriate Hong Kong Government Department or Registration Agency, HKCA or the Contractor may conduct a site visit the address of place of business to obtain documentation showing the Applicant's business, such as photos of a permanent signage, the exterior of the site, the interior reception area or workspace, etc.

In case of doubt, HKCA may decline the application.

3.2.3 Authentication of Individual Identity

Authentication of the identity of the Authorised Representative of Organisational Applicant will be accomplished through one of the processes as specified in Section 3.2.2.

3.2.4 Non-Verified Subscriber Information

HKCA verifies the subject elements and the alternative subject name as defined in Section 7.1.4.2 of the CA / Browser Forum Baseline Requirements.

3.2.5 Validation of Authority

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

For all applications of d-Cert (Server), the authority of the Authorised Representative is verified by using one or more of the procedures listed in Section 3.2.2.4 of the CA / Browser Forum Baseline Requirements ("BR") and a Reliable Method of Communication in accordance with Section 3.2.5 of the BR.

For EV d-Cert (Server), the authority of the Applicant is further verified in accordance with Section 11.8.3 of the CA / Browser Forum Extended Validation SSL certificate guidelines. In accordance with Section 11.5 of the same guidelines, HKCA shall ensure the telephone number and the email address provided in the application form as the Verified Method of Communication by sending an email with response from the Applicant to confirm that the Applicant can be contacted reliably by the telephone number provided and the Authorised Representative is authorised by the Applicant to submit the application of EV d-Cert(Server) on behalf of the Applicant.

3.2.6 Criteria for Interoperation

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

3.2.7 Authentication of Domain Names
HKCA validates the Applicant's ownership or control of each Fully-Qualified Domain Name ("FQDN") as stipulated in Section 4.2.1.

3.2.8 Authentication of IP Addresses
IP addresses are not supported for the d-Cert (Server) certificates.

3.3 Identification and Authentication for Re-Key Requests
HKCA 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
HKCA 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 HKCA's discretionary as part of a certificate replacement process.

3.3.2 Identification and Authentication for Re-Key After Revocation
HKCA shall not permit re-key of expired or revoked certificates.

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

3.4 Identification and Authentication for Revocation Request
After receiving the revocation request from subscriber or through the RA to which the request for revocation was first submitted, HKCA shall validate the request and verify the justifications for revocation. The certificate will be revoked, which terminates the validity of the certificate permanently, upon receipt of the final confirmation of revocation from the Subscriber or through the RA to which the request for revocation was first submitted. Such final confirmation of revocation can be (1) an action on a confirmation web page by the Subscriber, after having its identity authenticated in the designated web page on the HKCA website where the request was submitted, (2) an email digitally signed by the Subscriber's Private Key, (3) an original letter signed by the Subscriber or (4) a Request for Certificate Revocation Form signed by the Subscriber.

4. Certificate Life-Cycle Operational Requirements

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

4.1.1 Who Can Submit a Certificate Application
An Authorised Representative of Applicant that hold a valid business registration certificate issued by the Government of the Hong Kong SAR, statutory bodies of Hong Kong SAR whose

existence is recognized by the laws of Hong Kong, or bureaux, departments or agencies of Government of HKSAR may submit a certificate application to HKCA.

4.1.2 Enrolment Process and Responsibilities

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

a) Complete and submit their d-Cert applications either through the d-Cert Subscriber Portal, or through the Contractor or a RA
b) Provide required supporting documents as stated in the application form during the enrolment process,
c) Pay any applicable subscription fees,
d) Generate the Private Key and public key,
e) Generate the Certificate Signing Request (CSR) containing the public key and transmits the CSR to HKCA through a designated web page at https://www.hkca.hk.

By submitting a d-Cert application form, the Applicant authorises the publication of the d-Cert to any other person or in the HKCA Repository and thus accepts the d-Cert to be issued to the Applicant.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

The documentation required for proving the identity of the Subscriber Organisation and Authorised Representative(s) is stipulated in Sections 3.2.2 and 3.2.3 of this CPS. Upon satisfactory completion of the identity verification process, a secure link transmitted to Authorised Representative's designated email address for retrieval the PIN. Each such link will be valid for one (1) use only and will automatically expire one (1) calendar month from the date of issuance. Meanwhile, HKCA will check the Certification Authority Authorisation record(s) ("CAA Record") published for the domain name(s) to be identified in the certificate. If a CAA Record exists that does not list HKCA's domain names, neither "hkca.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, HKCA considers that the Applicant allows HKCA to issue certificate for the domain name(s).

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

a) Communicating directly with the Domain Name Registrant using an email address created by pre-pending 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' in the local part, followed by the at-sign ("@"), followed by the Authorisation Domain Name, which may be formed by pruning zero or more components from the requested FQDN (i.e. as stated in BR 3.2.2.4.4); or
b) Confirming the presence of a random value for either in a DNS CNAME, TXT or CAA record for either 1) an Authorisation Domain Name; or 2) an Authorisation Domain Name that is prefixed with a domain label that begins with an underscore character (i.e. as stated in BR 3.2.2.4.7); or
c) Validating that the Applicant, which is a Bureau or Department of the Government of Hong Kong SAR, is the domain contact if the Base Domain Name of the FQDN relates to the Government Entity (e.g. example.gov.hk) (i.e. as stated in BR 3.2.2.4.12); or

d) Confirming the presence of a random value within a file 1) located on the Authorization Domain Name, and 2) located under the "/.well-known/pki-validation" directory, and 3) retrieved via either the "http" or "https" scheme, and 4) accessed over an Authorized Port (i.e. as stated in BR 3.2.2.4.18).

4.2.2 Approval or Rejection of Certificate Applications

Following the identity verification process, HKCA has the obligation to notify Applicants of the approval or rejection of their applications. Applicants whose applications have been rejected may subsequently reapply. HKCA 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

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

Types of certificates	**Time periods for finishing the application**
DV d-Cert (Server)	Ten working days
OV d-Cert (Server)	Ten working days
EV d-Cert (Server)	Ten working days

For the avoidance of doubt, all Saturdays, Sundays, public holidays and for all weekdays on which a tropical cyclone warning signal no. 8 (or above) or a black rainstorm warning signal is hoisted, are not working days for the purpose of this Section 4.2.3.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

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

Upon receipt of the CSR, HKCA shall verify that the Applicant is in possession of the corresponding Private Key by checking the digital signature on the CSR structure containing the public key material. HKCA shall not have possession of the Applicants' Private Keys.

Upon verifying the Applicant's possession of his/her Private Key, HKCA shall generate the certificate in which the Applicant's public key will be included. To support Certificate Transparency in accordance with RFC 6962, HKCA shall submit the certificate to two or more Certificate Transparency Logs to obtain and attach the signed certificate timestamps (SCT) to the certificate.

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

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

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

The Applicant verifies and confirms the accuracy of the information contained in the d-Cert at the designated web page at https://www.hkca.hk. If the Applicant rejects the d-Cert, HKCA shall revoke that d-Cert. A Subscriber is deemed to have accepted the d-Cert when the Subscriber uses the d-Cert.

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

4.4.2 Publication of the Certificate by the CA

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

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

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

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subscribers are responsible for:

a) Undertaking an obligation to protect the confidentiality (i.e. keep it secret) and the integrity of their Private Key using reasonable precautions to prevent its loss, disclosure, or unauthorised use, and that they are responsible for any consequences under any circumstances for the compromise of the Private Key.
b) Reporting any loss or compromise of their Private Key immediately to HKCA upon discovery of the loss or compromise (a compromise is a security violation in which Information is exposed to potential unauthorised access, such that unauthorised disclosure, alteration, or use of the Information may have occurred).
c) Not using a certificate in a transaction on becoming aware of any ground upon which HKCA could revoke it under the terms of the CPS, or after the Subscriber has made a revocation request or been notified by HKCA of HKCA's intention to revoke the certificate under the terms of this CPS.
d) Upon becoming so aware of any ground upon which HKCA could revoke the certificate, or upon the Subscriber making a revocation request or upon being notified by HKCA 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 HKCA or at the Applicant's or Subscriber's request) and stating in clear terms that, as this is the case, the Relying Parties should not rely upon the certificate in respect of the transaction.
e) For the purpose of identity authentication, using the Private Key of a d-Cert only during its validity period.

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

4.5.2 Relying Party Public Key and Certificate Usage

Relying Parties relying upon d-Cert (Server) certificates are responsible for:

a) Relying on such certificates only when the reliance is reasonable and in good faith in light of all the circumstances known to the Relying Party at the time of the reliance.
b) Before relying upon a certificate determining that the use of the certificate and any digital signature supported by it is appropriate for its purposes under this CPS while the Contractor or RA (if any, see **Appendix F**) does not undertake any duty of care to Relying Parties at all.
c) Checking the status of the certificate on the certificate revocation list, or the relevant OCSP response whenever applicable, prior to reliance.
d) Performing all appropriate certificate path validation procedures.
e) After validity period of the certificate, only using its Public Key for signature verification.

4.6 Certificate Renewal

4.6.1 Circumstances for Certificate Renewal

HKCA shall notify Subscribers to renew their d-Cert (Server) certificates prior to the expiry of the certificates. The certificates can be renewed before expiry of their validity at the request of the Subscriber and the discretion of HKCA. HKCA shall not perform renewal of expired or revoked certificates. At the discretion of HKCA, the validity period of the new certificate to be issued to the Subscriber may vary from the period stated for the certificate specified in Section 6.3.2, and span up to 199 days:

Validity period of a new certificate	**Validity period start date to be specified in the new certificate**	**Validity period end date to be specified in the new certificate**	**Remarks**
Up to 199 days	The date the new certificate is generated	199 days after the date the new certificate is generated, or the subscription end date, whichever is earlier.	The validity period of the new certificate may vary and span up to 199 days

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

4.6.2 Who May Request Renewal

There is no automatic certificate renewal of a d-Cert (Server) certificates. The process of "Authentication of Organisation Identity" as described under Section 3.2.2 of this CPS will be conducted. The Authorised Representative of the organisation will need to complete and submit a Certificate Renewal Form (available at HKCA web site at https://www.hkca.hk) along with the other documentation referred to in the application form and appropriate renewal fee. In circumstances where Authorised Representatives are replaced, the new Authorised Representative will need to also complete and submit an application form as specified in Section 3.2.2 (a).

4.6.3 Processing Certificate Renewal Requests

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

4.6.4 Notification of New Certificate Issuance to Subscriber
Notification to the Subscriber about the issuance of a renewed certificate is given using the same means as a new d-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 d-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

HKCA publishes a renewed d-Cert in the same way as a new d-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 HKCA's discretionary as part of a certificate replacement process.

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

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

4.7.4 Notification of New Certificate Issuance to Subscriber
HKCA 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
HKCA publishes a re-keyed d-Cert in the same way as a new d-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 d-Cert.

4.8.1 Circumstances for Certificate Modification
No stipulation.

4.8.2 Who May Request Certificate Modification
No stipulation.

4.8.3 Processing Certificate Modification Requests
No stipulation.

4.8.4 Notification of New Certificate Issuance to Subscriber
No stipulation.

4.8.5 Conduct Constituting Acceptance of Modified Certificate
No stipulation.

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

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

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

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

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

4.9.1 Circumstances for Revocation
Each Subscriber MUST apply to HKCA 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 a d-Cert has been, or is suspected of having been, compromised or any change in the Information in the certificate provided by the Subscriber.

HKCA will revoke a d-Cert (Server) in accordance with the procedures in the CPS within 24 hours whenever it:

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

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

HKCA may revoke a d-Cert (Server) within 24 hours and will revoke a d-Cert (Server) within 5 days in accordance with the procedures in the CPS whenever it:

6) receives a request for revocation of a d-Cert (Server) by letter mail, email, in-person from a Subscriber;
7) determines that a d-Cert (Server) no longer complies with the requirements of Sections 6.1.5 and 6.1.6 of the CA/Browser Forum baseline requirements in relation to key sizes and public key parameter generation and quality checking;
8) obtains evidence that a d-Cert (Server) was misused;
9) determines that the Subscriber had failed to meet any of the obligations set out in this CPS or the Subscriber Agreement;
10) knows or reasonably suspects any circumstance indicating that use of a FQDN in the d-Cert (Server) is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name registrant and the Applicant has terminated, or the Domain Name registrant has failed to renew the Domain Name);
11) knows or reasonably suspects that a Wildcard d-Cert (Server) has been used to authenticate a fraudulently misleading subordinate FQDN;
12) knows or reasonably suspects a material change in the information contained in a d-Cert (Server);
13) determines that a d-Cert (Server) was not properly issued in accordance with the CA/Browser Forum baseline requirements or this CPS;
14) determines, or knows or reasonably suspects that any of the information appearing in a d-Cert (Server) is inaccurate;
15) is required to do so when HKCA's right to issue certificate under CA/Browser Forum baseline requirements expires or is revoked or terminated, unless HKCA has made arrangements to continue maintaining the CRL and/or OCSP repository;
16) is required to do so by this CPS, any regulation, or law applicable to the d-Cert (Server) ;
17) determines that the Subscriber has failed to pay the subscription fee;
18) determines that 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;
19) knows or has reasonable cause to believe that any of the server name identified in the Subject Name or Subject Alternative Name, if any, in a d-Cert (Server) is no longer owned by the Subscriber Organisation; or
20) knows or has reasonable cause to believe that the Subscriber whose details appear on a d-Cert (Server) that:

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

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

1) HKCA obtains evidence that the Sub CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Sections 6.1.5 and 6.1.6 of the CA/Browser Forum baseline requirements in relation to key sizes and public key parameter generation and quality checking;
2) HKCA obtains evidence that the Sub CA Certificate was misused;
3) HKCA confirms that the Sub CA Certificate was not issued in accordance with the CA/Browser Forum baseline requirements or this CPS;
4) HKCA determines that any of the information appearing in the CA Certificate is inaccurate or misleading;
5) HKCA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the CA Certificate;
6) HKCA's right to issue Certificates under the Baseline Requirements expires or is revoked or terminated, unless HKCA has made arrangements to continue maintaining the CRL/OCSP Repository;
7) Revocation is required by HKCA's CPS; or
8) The technical content or format of the Sub CA Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties.

4.9.2 Who Can Request Revocation

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

4.9.3 Procedure for Revocation Request

After receiving the revocation request, HKCA shall validate the request and verify the justifications for revocation. The certificate will be revoked, which terminates the validity of the certificate permanently, upon receipt of the final confirmation of revocation from the Subscriber or through the RA to which the request for revocation was first submitted. Such final confirmation of revocation can be (1) an action on a confirmation web page by the Subscriber, after having its identity authenticated in the designated web page on the HKCA website where the request was submitted, (2) an email digitally signed by the Subscriber's Private Key, (3) an original letter signed by the Subscriber or (4) a Request for Certificate Revocation Form signed by the Subscriber. HKCA will notify the Subscriber by updating the certificate revocation list, or by updating the relevant OCSP response whenever applicable and by email, if a contact email address is available, of such revocation ("Notice of Revocation") in accordance with the procedures in the CPS. If the certificate supports OCSP, the OCSP response for that certificate will remain revoked after the certificate expires. The Request for Certificate Revocation Form can be obtained from the web site at https://www.hkca.hk.

The HKCA business hours for processing certificate revocation requests submitted by email or in-person are as follows:

Monday - Friday	09:00 am - 5:00 pm

Saturday, Sunday & Public Holiday	No service

If a Tropical Cyclone Warning Signal No. 8 (or higher) or a Black Rainstorm Warning Signal is hoisted, processing of revocation requests will be suspended immediately. Processing will resume as follows:

- If the signal is lowered at or before 6:00 a.m. on the same day, processing will recommence at the service's usual business hours that day.
- If the signal is lowered after 6:00 a.m. but at or before 10:00 a.m., processing will recommence at 2:00 p.m. on that day, provided the day is not a Saturday, Sunday or public holiday.
- If the signal is lowered after 10:00 a.m., processing will recommence at the usual business hours on the next weekday that is not a Saturday, Sunday or public holiday.

4.9.4 Revocation Request Grace Period

The revocation request grace period ("Grace Period") means the period during which the Subscriber must make a revocation request. Each Subscriber MUST apply to HKCA 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 a d-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 HKCA 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 HKCA of HKCA's intention to revoke the certificate. HKCA 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 HKCA could revoke the certificate, or upon making a revocation request or upon being notified by HKCA 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 HKCA 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. HKCA 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.

HKCA shall be under no liability to Relying Parties in respect of the transactions in the period between HKCA's decision to revoke a certificate (either in response to a request or otherwise) and the appearance of the revocation status on the Certificate Revocation List, or in the period between that decision to revoke a certificate and the update of the relevant OCSP response, unless HKCA has failed to exercise reasonable skill and care and the Subscriber has failed to notify the Relying Party as required by these provisions. Any such liability is limited as set out elsewhere in this CPS. In no circumstances does the RA itself undertake a separate duty of care to Relying Parties (the RA is simply discharging HKCA's duty of care), and accordingly, even if negligent, the RA itself cannot be held liable to Relying Parties.

4.9.5 Time within Which CA Must Process the Revocation Request

For submission of certificate revocation request to HKCA through a designated web page on the HKCA web site, the revocation would be reflected in CRL within 24 hours. For requests by other methods, HKCA 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 HKCA to revoke the certificate, the revocation is posted to the Certificate Revocation List. However, a Certificate Revocation List is not immediately published in the directory for access by the public following each certificate revocation. Only when the next Certificate Revocation List is updated and published will it reflect the revoked status of the certificate. Certificate Revocation Lists are published 3 times daily and are archived for at least 7 years. On the contrary, if the certificate supports OCSP, the OCSP response for that certificate will be updated and published immediately to reflect the revocation status of that certificate.

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

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

Each Relying Party making use of a HKCA 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.

HKCA'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 a d-Cert is revoked, HKCA shall publish the relevant information (including the Certificate Revocation List (such as Authority Revocation List of HKCA) on a timely basis.

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

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

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

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

4.9.11 Other Forms of Revocation Advertisements Available
No stipulation.

4.9.12 Special Requirements Related to Key Compromise
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 HKCA web site, with reason "key compromise" to HKCA. If HKCA 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 HKCA 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 HKCA" and verifiable by the Public Key of a valid certificate maintained in the Repository of HKCA; or
b) the Private Key itself.

4.9.13 Circumstances for Suspension
Not applicable.

4.9.14 Who Can Request Suspension
Not applicable.

4.9.15 Procedure for Suspension Request
Not applicable.

4.9.16 Limits on Suspension Period
Not applicable.

4.10 Certificate Status Services

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

4.10.2 Service Availability
Certificate status services are available 24x7.

4.10.3 Operational Features
No stipulation.

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

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

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

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

HKCA 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 HKCA Private Keys and Subscribers' Private Keys in the d-Cert system used by HKCA.

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 HKCA operation is located in a site that affords commercially reasonable physical security. During construction of the site, HKCA took appropriate precautions to prepare the site for CA operations.

5.1.2 Physical Access
HKCA 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, HKCA 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 HKCA's control) used in connection with providing the HKCA 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. HKCA 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.

5.1.7 Waste Disposal
HKCA 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
HKCA has established backup systems for critical systems (including HKCA 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 HKCA, of the Contractor and of RAs acting on behalf of HKCA (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 HKCA'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 HKCA's CA operation.

5.2.2 Number of Personnel Needed for Each Task
HKCA Private keys are stored in tamper-proof hardware cryptographic devices. HKCA implements multi-person control (3 out of 5 multi-person control) over the activation, usage, deactivation of HKCA 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 HKCA d-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
HKCA 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 HKCA, 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
HKCA 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 HKCA'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
HKCA, the Contractor or its RAs shall ensure all their staff (including those assuming the

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

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

5.3.4 Retraining Frequency and Requirements
HKCA, the Contractor or its RAs shall provide appropriate and sufficient training for their staff (at least once a year for those holding core positions) to ensure their capabilities in carrying their duties as well as effective implementation and compliance with security policies.

5.3.5 Job Rotation Frequency and Sequence
No stipulation

5.3.6 Sanctions for Unauthorised Actions
HKCA, 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
HKCA 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 HKCA, the Contractor and RAs are delivered in a control and secure manner using a protocol prescribed by HKCA from time to time.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded
Significant security events in the HKCA 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;
- Signing of OCSP responses; 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;
- Generation of CRLs; and
- Signing of OCSP responses.

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 HKCA.

5.4.3 Retention Period for Audit Log
Archived audit log files are retained for at least 10 years.

5.4.4 Protection of Audit Log
HKCA 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)
HKCA 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
HKCA 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 HKCA's CA security procedures.

5.5 Records Archival

5.5.1 Types of Records Archived
HKCA 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) HKCA:

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 HKCA is bound;
e) All certificates and CRLs as issued or published, and all OCSP responses;
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 10 years. Audit trail files are maintained in the CA system as deemed appropriate by HKCA.

5.5.3 Protection of Archive
Archived media maintained by HKCA 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. HKCA shall verify the consistency of archival records during the archival process. During the archival period, HKCA 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. HKCA 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 HKCA.

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 HKCA and d-Cert root keys and certificates created by HKCA (See

Appendix H) for the purpose of certifying certificates issued under this CPS is no more than 25 years. HKCA 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 HKCA web site https://www.hkca.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. HKCA 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

HKCA 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, HKCA implements, documents, and periodically tests appropriate contingency and disaster recovery plans and procedures.

HKCA 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, HKCA 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 HKCA Private Key for the issuance of d-Cert (Server) certificates under this CPS has been compromised or damaged, HKCA 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 HKCA on behalf of the Subscriber has been compromised or damaged, HKCA shall promptly revoke the respective certificates and issue new and replacement certificates. HKCA 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.

HKCA shall promptly notify the Commissioner for Digital Policy and make public announcement if a HKCA Private Key for the issuance of d-Cert (Server) certificates under this CPS has been compromised. The compromise of a HKCA Private Key will result in prompt revocation of the certificates issued under that Private Key and the issuance of new and replacement certificates. HKCA 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 HKCA Private Key for the issuance of d-Cert (Server) certificates under this CPS has been compromised or corrupted and cannot be recovered, HKCA shall promptly notify the Commissioner for Digital Policy and make a public announcement as to which certificates have been revoked, and how the new HKCA Public Key is provided to Subscribers, and how Subscribers are issued with new certificates. In case of revocation requests for the HKCA root certificate, HKCA 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 HKCA 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.

HKCA 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 HKCA 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 HKCA termination plan. Upon termination of service, HKCA 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 HKCA is withdrawn, the d-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 HKCA to specifically protect its cryptographic keys and associated data. Control of HKCA keys is implemented through physical security and secure key storage. The HKCA keys are generated, stored, used and destructed only within a tamper-proof hardware device, which is under multi-person access control.

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Key pairs for HKCA and Applicants/Subscribers are generated through a procedure such that the Private Key cannot be accessed by anyone other than the authorised user of the Private Key unless there is some compromise of the procedure by the authorised user. HKCA generates the root CA and Sub CA key pairs for issuing certificates that conform to this CPS.

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

For root CA key pairs, HKCA 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 HKCA followed its 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

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

6.1.3 Public Key Delivery to Certificate Issuer

The Applicant's Public Key which will be generated by the Applicant must be transferred to HKCA using a method designed to ensure that:

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

6.1.4 CA Public Key Delivery to Relying Parties

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

6.1.5 Key Sizes

HKCA employs the following RSA key sizes and hash algorithms for its Root CA certificates, Subordinate CA certificates and subscriber certificates. All certificate types must comply with the algorithm and key size requirements specified below.

Certificate Type	Digest Algorithm	Minimum RSA Modulus Size (bits)
Root CA certificate	SHA-256	4096
Sub CA certificate	SHA-256	2048
Subscriber Certificate	SHA-256	2048

6.1.6 Public Key Parameters Generation and Quality Checking

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

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

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

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

The cryptographic devices used by HKCA are rated to at least FIPS 140-2 Level 3.

6.2.2 Private Key (n out of m) Multi-Person Control

HKCA Private Keys are stored in tamper-proof hardware cryptographic devices. HKCA implements multi-person control (3 out of 5 multi-person control) over the activation, usage, deactivation of HKCA Private Keys.

6.2.3 Private Key Escrow

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

6.2.4 Private Key Backup

Each HKCA 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 HKCA 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 HKCA 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, HKCA has implemented strict key management processes for controls of Private Keys transfer in order to protect the HKCA Private Keys from being lost, stolen, tampered, disclosed or used without authorisation.

6.2.7 Private Key Storage on Cryptographic Module

HKCA 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

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

OCSP signing operations are performed in a hardware cryptographic module. Archival of HKCA 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.

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

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

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

Certificates issued under this CPS to new applicants shall have a validity period of 199 days.

Certificates issued under this CPS as part of a renewal process may be valid for a period different from the respective validity period listed above (see Section 4.6). The effective and expiration dates defining the validity period of each certificate are stated within 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
HKCA Private Keys are stored in tamper-proof hardware cryptographic devices. HKCA implements multi-person control (3 out of 5 multi-person control) over the activation, usage, deactivation of HKCA Private Keys.

6.4.2 Activation Data Protection
HKCA Private Keys are stored in tamper-proof hardware cryptographic devices. HKCA implements multi-person control (3 out of 5 multi-person control) over the activation, usage, deactivation of HKCA 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
HKCA 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. HKCA implements stringent management mechanism to control and monitor the operating systems, in order to prevent unauthorised modification. When processing disposal of waste devices, HKCA will exercise reasonable endeavours to erase their storage with confirmation for which may contain information related to the security of d-Cert service.

6.5.2 Computer Security Rating
No stipulation

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls
HKCA implements controls over the procedures for the procurement and development of software and hardware for HKCA 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 HKCA 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 HKCA's hardware cryptographic devices throughout their lifecycle (from the commissioning of these devices to their logical/physical destruction).

6.6.2 Security Management Controls
HKCA 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
HKCA shall implement security measures such as multi-level firewall, intrusion detection system, security audit, anti-virus system to protect the HKCA'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.

HKCA 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, HKCA shall assess the associated risks, create and implement a documented mitigation plan.

6.8 Time-Stamping

The system time on HKCA'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). HKCA 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 d-Cert (Server) certificates is in **Appendix E**.

HKCA 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

HKCA updates and publishes the following Certificate Revocation Lists (CRLs) containing information of d-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 a d-Cert (Server) certificate 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

Revocation reason	Revocation reason code (CRLReason as specified in RFC5280)
	(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 HKCA 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:

- HKCA obtains verifiable evidence that the certificate subscriber's private key corresponding to the public key in the certificate suffered a key compromise; or
- HKCA 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
- HKCA 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 HKCA 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 HKCA web site as set out in Section 4.9.12 of this CPS, then HKCA will revoke all instances of that key across all subscribers.

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

When HKCA 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, HKCA may update the CRL entry to enter "keyCompromise" as the revocation reason code in the reason code extension. Additionally, HKCA 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:

- HKCA obtains evidence that the certificate was misused; or
- HKCA 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
- HKCA is made aware that a d-Cert (Server) with Wildcard feature has been used to authenticate a fraudulently misleading subordinate fully-qualified domain name; or
- HKCA is made aware of a material change in the information contained in the certificate; or
- HKCA determines or is made aware that any of the information appearing in the certificate is inaccurate; or
- HKCA 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
- HKCA 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
- HKCA 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
- HKCA 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
- HKCA 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
- HKCA 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
- HKCA 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 HKCA 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

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

Root CA

Certificate subject name (CN)	**OCSP signer's certificate subject name (CN)**
"HKCA Root CA 2"	"HKCA Root CA 2 OCSP Responder"

Sub CA

Certificate subject name (CN)	**OCSP signer's certificate subject name (CN)**
"HKCA d-Cert DV SSL CA 2 - 25"	"HKCA d-Cert DV SSL CA 2 - 25 OCSP Responder"
"HKCA d-Cert OV SSL CA 2 - 25"	"HKCA d-Cert OV SSL CA 2 – 25 OCSP Responder"
"HKCA d-Cert EV SSL CA 2 - 25"	"HKCA d-Cert EV SSL CA 2 - 25 OCSP Responder"

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

7.3.1 Version Number(s)

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

7.3.2 OCSP Extensions

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

8. Compliance Audit and Other Assessments

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

8.1 Frequency and Circumstances of Assessment

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

8.2 Identity/Qualifications of Assessor

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

8.3 Assessor's Relationship to Assessed Entity

Compliance assessments are performed by an independent external auditor that is independent from HKCA 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 HKCA's system of issuing, revoking and publishing d-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 HKCA's services, then (1) the auditor will document the discrepancy, (2) the auditor will promptly notify HKCA, and (3) depending on the nature and extent of the discrepancy, HKCA will create a suitable corrective action plan to cure the noncompliance and decide whether to take any remedial action with regard to d-Certs already issued.

8.6 Communications of Results

WebTrust for Certification Authorities audit report is made available to the public at https://www.hkca.hk/cps. 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, HKCA performs self-audits against a randomly selected sample of at least 3 percent of the d-Certs issued since the last self-audit. Self-audits on d-Certs are performed in accordance with guidelines adopted by the CA / Browser Forum.

9. Other Business and Legal Matters

9.1 Fees

HKCA may periodically determine its charges for processing new and renewal application for d-Certs, revocation requests, administration, and any other d-Cert-related services. A schedule of the current fees is available on the HKCA website. HKCA reserves its right to change this fee schedule from time to time and may publish it through other means as well.

All applicable charges must be paid in full before the commencement of each subscription period (see section 3.2) by d-Cert Subscribers, unless waived by HKCA. HKCA may suspend or revoke a d-Cert if its subscription terminates during the validity period specified in the certificate (see also section 4.5.1.4(f)).

Within the one-year subscription period, d-Cert (Server) subscribers will be eligible to obtain an unlimited number of new certificates under the same application at no additional charge. The validity period of each new certificate will comply with the phased maximum validity period or reflect the remaining subscription period, whichever is shorter.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

HKCA maintains commercial general liability insurance coverage of at least two million US dollars and the professional liability/errors and omissions insurance of at least five million US dollars as specified in the CA / Browser Forum Extended Validation SSL certificate guidelines. Moreover, a separate insurance policy is also in place to cover the potential or actual liabilities and claims against Reliance Limit on the certificates pursuant to the provisions of ETO.

9.2.2 Other Assets

No stipulation

9.2.3 Insurance or Warranty Coverage for End-Entities

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

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

Information about Subscribers that is submitted as part of an application for a d-Cert (Server) certificate under this CPS will be used only for the purposes collected and is kept confidential except to the extent necessary for HKCA or the Contractor to perform HKCA'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

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

such record, book, register, correspondence, information, document or other material to any other person.

Such Information will not be released without the prior consent of the Subscriber except when required by a court-issued subpoena or order, or when otherwise required by the laws of Hong Kong SAR. HKCA 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
HKCA has implemented a privacy policy, which complies with this CPS. The HKCA privacy policy is published at HKCA web site at https://www.hkca.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
HKCA shall ensure that the restrictions in this subsection will be adhered to by itself and any persons of HKCA, the Contractor, RAs and any HKCA subcontractors, who have access to any record, book, register, correspondence, information, document or other material in performing tasks related to HKCA's system of issuing, revoking and publishing d-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 a d-Cert (Server) certificate under this CPS will be used only for the purposes collected and is kept confidential except to the extent necessary for HKCA or the Contractor to perform HKCA's obligations under this CPS.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process
Such Information will not be released without the prior consent of the Subscriber except when required by a court-issued subpoena or order, or when otherwise required by the laws of Hong Kong SAR. HKCA 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
HKCA owns all intellectual property rights associated with its databases, web sites, d-Cert certificates, trademarks and any other publication originating from HKCA 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 HKCA.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

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

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

9.6.2 RA Representations and Warranties

Registration Authorities (RAs) are responsible only to HKCA under the terms of the agreement (the "RA Agreement") under which they are appointed by HKCA as its agents to carry out on HKCA's behalf certain of HKCA's obligations as detailed in this CPS. RAs, on behalf of HKCA, collect and keep documents and information supplied under the terms of the CPS and Subscriber Agreements. HKCA 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 HKCA.

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

9.6.3 Subscriber Representations and Warranties

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

a) No person other than the Subscriber of a d-Cert (Server) certificate has had access to the Subscriber's Private Key.
b) Each Digital Signature generated using the Subscriber's Private Key, which corresponds to the Public Key contained in the Subscriber's d-Cert, is the Digital Signature of the Subscriber.
c) A d-Cert (Server) certificate is to be used only for the purposes stipulated in Section 1.4.

d) All information and representations made by the Subscriber included in the certificate are true.
e) The certificate will be used exclusively for authorised and legal purposes consistent with this CPS.
f) All information supplied in the certificate application process does not infringe or violate in any way the trademarks, service marks, trade name, company name, or any other intellectual property rights of any third party.

Subscribers are responsible for:

a) Completing the application procedures properly and signing, or confirming acceptance of, a Subscriber Agreement by the Authorised Representative in the appropriate form and performing the obligations placed upon them by that Agreement, and ensuring accuracy of representations in certificate application.
b) Accurately following the procedures specified in this CPS as to the expiry of certificates.
c) Notifying HKCA immediately from time to time of any change in the appointment and information of the Authorised Representative of d-Cert (Server) certificates.
d) Notifying HKCA immediately of any fact which may give rise to HKCA, 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 HKCA could revoke it under the terms of the CPS, or after the Subscriber has made a revocation request or been notified by HKCA of HKCA's intention to revoke the certificate under the terms of this CPS.
f) Upon becoming so aware of any ground upon which HKCA could revoke the certificate, or upon the Subscriber making a revocation request or upon being notified by HKCA 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 HKCA 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 a d-Cert application form, they authorise the publication of the d-Cert to any other person or in the HKCA's Repository.
h) For the purpose of identity authentication, using the Private Key of a d-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 HKCA 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 d-Cert (Server) certificates are responsible for:

a) Relying on such certificates only when the reliance is reasonable and in good faith in light of all the circumstances known to the Relying Party at the time of the reliance.
b) Before relying upon a certificate determining that the use of the certificate and any digital signature supported by it is appropriate for its purposes under this CPS while the Contractor or RA (if any, see **Appendix F**) does not undertake any duty of care to Relying Parties at all.
c) Checking the status of the certificate on the certificate revocation list, or the relevant OCSP response whenever applicable, prior to reliance.
d) Performing all appropriate certificate path validation procedures.
e) After validity period of the certificate, only using its Public Key for signature verification.

9.6.5 Representations and Warranties of Other Participants

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

9.7 Disclaimers of Warranties

HKCA undertakes to each Subscriber and to each Relying Party that a reasonable degree of skill and care will be exercised by HKCA, by the Contractor and by the RA when acting on behalf of HKCA in performing the obligations and exercising the rights it has as a CA set out in this CPS. **HKCA 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 HKCA, or the officers, employees or agents of HKCA 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 HKCA, by the Contractor or by the RA acting on behalf of HKCA 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 the HKCA, 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 HKCA, the Contractor or the RA acting on HKCA's behalf has exercised a reasonable degree of skill and care, the HKCA, 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 HKCA.

This means, also, that, provided HKCA (by the HKCA, the Contractor or the RA acting on behalf of HKCA) has exercised a reasonable degree of skill and care to avoid and/or mitigate the effects of matters beyond its control, neither the HKCA, the Contractor nor any such RA is liable for the adverse effects to Subscribers or Relying Parties of any matters outside HKCA'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 HKCA, the Contractor nor any RA acting on behalf of HKCA 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 HKCA, the Contractor or any RA acting on HKCA'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 HKCA to limit its liabilities as set out in the Subscriber Agreement and in this CPS.

In the event of HKCA's breach of:

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

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

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

Subject to the exceptions that appear below, in the event of HKCA's breach of:

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

the liability of HKCA to any Subscriber and any Relying Party, whether as Subscriber or Relying Party as defined by the CPS or in any other capacity at all, is limited to, and shall not under any circumstances exceed, HK$200,000 in respect of one OV or EV d-Cert (Server) certificate, or HK$0 (zero) in respect of one DV d-Cert (Server) certificate.

Any Subscriber or Relying Party who wishes to make any legal claim upon HKCA arising out of or in any way connected with the issuance, revocation or publication of a d-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 HKCA, the Contractor nor any RA nor any officer or employee or other agent of the HKCA, the Contractor, or any RA is to be a party to the Subscriber Agreement, and the Subscriber and Relying Parties must acknowledge to HKCA that, as far as the Subscriber and Relying Parties are aware, neither the HKCA, 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 HKCA of a Subscriber Agreement or any certificate issued by HKCA as a CA and each and every Subscriber and Relying Party accepts and will continue to accept that and undertakes to HKCA 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 HKCA of a Subscriber Agreement or any certificate issued by HKCA as a CA and acknowledges that HKCA has a sufficient legal and financial interest to protect these organisations and individuals from such actions.

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

9.9 Indemnities

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

> *"The HKCA acting by its officers 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 HKCA'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 d-Certs which may be read on the HKCA web site at https://www.hkca.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 HKCA (by the HKCA, the Contractor and their respective officers, employees and agents) issues this certificate without undertaking any responsibility or duty of care to Relying Parties save as set out in the CPS.*
>
> *Relying Parties, before relying upon this certificate are responsible for:*
>
> a. *Relying on it only when reliance is reasonable and in good faith in the light of all the circumstances known to the Relying Party at the time of reliance;*
> b. *Before relying upon this certificate, determining that the use of the certificate and any digital signature supported by it is appropriate for its purposes under the CPS;*
> c. *Checking the status of this certificate on the Certificate Revocation List, or the relevant OCSP response whenever applicable, prior to reliance; and*
> d. *Performing all appropriate certificate path validation procedures.*
>
> *If, despite the exercise of reasonable skill and care by the HKCA, the Contractor and their respective officers, employees or agents, this certificate is in any way inaccurate or misleading, the HKCA, the Contractor and their respective officers, employees or agents, accept no responsibility for any loss or damage to the Relying Parties and the applicable Reliance Limit that applies to this certificate under the Ordinance in these circumstances is HK$0.*

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

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

Time Limit For Making Claims
Any Relying Party who wishes to make any legal claim upon the HKCA arising out of or in any way connected with the issuance, revocation or publication of this d-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 HKCA, 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 HKCA in the HKCA website at https://www.hkca.hk/cps or in the HKCA Repository and are binding on all current and subsequent Applicants and Subscribers to whom certificates are issued.

HKCA 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 HKCA 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 HKCA termination plan. Upon termination of service, HKCA 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 HKCA pertaining to matters within the scope of this CPS are final. Any claims should be submitted to HKCA at the following address:

Hong Kong Internet Registration Corporation Limited
Unit 501, Level 5, Core C, Cyberport 3, 100 Cyberport Road, Hong Kong
Email: enquiry@hkca.hk

9.12 Amendments

9.12.1 Procedure for Amendment

Upon approval of an updated CPS by HKCA, the CPS changes will be effective upon publication by HKCA in the HKCA web site at https://www.hkca.hk or in the HKCA 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 HKCA. In the event of a conflict between this CPS and the Subscriber Agreement, other rules, guidelines, or contracts, the Subscriber, Relying Parties and HKCA 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

HKCA 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 HKCA web site at https://www.hkca.hk.

9.12.3 Circumstances Under Which OID Must be Changed

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

9.13 Dispute Resolution Provisions

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

Hong Kong Internet Registration Corporation Limited
Unit 501, Level 5, Core C, Cyberport 3, 100 Cyberport Road, Hong Kong
Email: enquiry@hkca.hk

9.14 Governing Law

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

9.15 Compliance with Applicable Law

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

9.16 Miscellaneous Provisions

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

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

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

9.16.4 Enforcement (Attorney's Fees and Waiver of Rights)
The decisions of HKCA pertaining to matters within the scope of this CPS are final. Any claims should be submitted to HKCA at the following address:

Hong Kong Internet Registration Corporation Limited
Unit 501, Level 5, Core C, Cyberport 3, 100 Cyberport Road, Hong Kong
Email: enquiry@hkca.hk

9.16.5 Force Majeure
HKCA 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 HKCA 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 HKCA, 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. HKCA agrees to transfer those articles into possession of Applicants or Subscribers for the limited purposes set out in this CPS. Nonetheless HKCA 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 HKCA's liability shall be as set out in Section 9.8. In addition, the articles transferred from HKCA may contain other material not relevant to the completion and acceptance of a d-Cert, if it does, the legal position in relation to such material is not governed by the CPS or the Subscriber Agreement, but by separate terms and conditions that will be referred to in the terms and conditions enclosed in the articles.

Appendix A – Glossary and Acronyms

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

"Accept", in relation to a certificate

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

(i) confirm the accuracy of the information on the person as contained in the certificate;

(ii) authorise the publication of the certificate to any other person or in a repository;

(iii) use the certificate; or

(iv) otherwise demonstrate the approval of the certificate; or

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

(i) confirm the accuracy of the information on the person that is to be contained in the certificate;

(ii) authorise the publication of the certificate to any other person or in a repository; or

(iii) otherwise demonstrate the approval of the certificate;

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

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

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

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

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

"Business Entity" means any Subscriber Organisation that is not a Private Organisation, Government Entity, or Non-Commercial Entity as defined in the CA / Browser Forum Extended Validation SSL certificate guidelines. The Subscriber Organisation is not a limited company and only has the Business Registration (BR) issued by the Inland Revenue Department of the Government of Hong Kong SAR.

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

"CA" means Certification Authority.

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

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

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

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

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

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

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

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

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

"**Compromised Key Reporting web page**" is a web page in HKCA website for reporting of suspected Private Key Compromise related to Certificates.

"Contract" means the outsourcing contract that HKCA has awarded to the Contractor for operating and maintaining the systems and services of the HKCA as stipulated in this CPS on behalf of HKCA.

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

"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).

"Domain Validation" in relation to HKCA d-Cert (Server) supporting Domain Validation, means a certificate that contains subject information specified in the CA / Browser Forum Baseline Requirements for Domain Validated (DV) certificates, and for which the Applicant's control over the domain has been validated in accordance with the CA / Browser Forum Baseline Requirements.

"d-Cert Subscriber Portal" means the web-based platform maintained by HKCA for Subscribers to create accounts, submit certificate applications, make payments, and manage their d-Cert certificates.

"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.

"Extended Validation" in relation to HKCA d-Cert (Server) supporting Extended Validation, means a certificate that contains subject information specified in the CA / Browser Forum Extended Validation SSL certificate guidelines and for which the Applicant's identity and domain ownership have been validated in accordance with the CA / Browser Forum Extended Validation SSL certificate guidelines.

"Extended Validation SSL certificate guidelines" means the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates published at https://www.cabforum.org.

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

"Government Entity", as defined in the CA / Browser Forum Extended Validation SSL certificate guidelines, means a Bureau or Department of the Government of Hong Kong SAR.

"HKID Card" means the Hong Kong Identity 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.

"Incorporating Agency", in relation to EV d-Cert (Server)

(a) in the context of a Private Organisation, means the Companies Registry of the Government of Hong Kong SAR (see https://www.cr.gov.hk/) under whose authority the legal existence of the entity is registered; or

(b) in the context of a Government Entity, means the entity that enacts law, regulations, or decrees of Hong Kong SAR establishing the legal existence of Government Entities.

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

"Information System" means a system which -

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

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

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

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

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

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

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

"Notary" means a solicitor holding a current certificate of appointment and is registered on the Register of Notaries Public kept by the Registrar of the High Court of Hong Kong.

"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 d-Cert.

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

"Organisation Validation" in relation to HKCA d-Cert (Server) supporting Organisation Validation, means a certificate that contains subject information specified in the CA / Browser Forum Baseline Requirements for Organisation Validated (OV) certificates, and for which the Applicant's organizational identity and domain ownership have been validated in accordance with the CA / Browser Forum Baseline Requirements.

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

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

"Practising Certified Public Accountant" means a certified public accountant holding a current practising certificate issued under the Professional Accountants Ordinance (Cap. 50).

"Practising Solicitor" means a solicitor holding a current practicing certificate and is enrolled on the Roll of Solicitors kept by the Registrar of the High Court of Hong Kong.

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

"Private Organisation", as defined in the CA / Browser Forum Extended Validation SSL certificate guidelines, means any Subscriber Organisation that has both Certificate of Incorporation (CI) issued by the Companies Registry and a Business Registration (BR) issued by the Inland Revenue Department of the Government of Hong Kong SAR, or any statutory body of Hong Kong SAR whose existence is recognized by the Laws of Hong Kong SAR.

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

"RA" means Registration Authority.

"Recognized CA" means Recognized Certification Authority.

"Recognized Certificate" means

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

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

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

"Registration Agency" means the Inland Revenue Department of the Government of Hong Kong SAR (see https://www.ird.gov.hk/) that registers business information in connection with an entity's business formation or authorisation to conduct business under a license, charter or other certification.

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

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

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

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

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

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

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

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

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

"SSL" is the acronym of Secure Sockets Layer.

"Sub CA" means the subordinate Certification Authority certificate which is issued by the root CAs of HKCA and is used to sign the HKCA Recognized Certificates.

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

"Subscriber" means a person who:

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

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

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

"Subscription Period" means the one-year period during which d-Cert (Server) subscribers will be eligible to obtain an unlimited number of new certificates under the same application at no additional charge.

"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.

"Verified Professional Letter" means a verified accountant letter or verified legal opinion as specified in the CA / Browser Forum Extended Validation SSL certificate guidelines.

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

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

For the purpose of the Electronic Transactions Ordinance, a Digital Signature is taken to be supported by a Certificate if the Digital Signature is verifiable with reference to the Public Key listed in a Certificate the Subscriber of which is the signer.

Appendix B - HKCA d-Cert Format

This appendix provides the formats of d-Cert issued by the Sub CAs "HKCA d-Cert DV SSL CA 2 - 25", "HKCA d-Cert OV SSL CA 2 - 25" and "HKCA d-Cert EV SSL CA 2 - 25" under this CPS. For the format of d-Cert issued by the other Sub CA(s) of HKCA or issued under other CPS, please refer to the prevailing CPS in respect of the issuance date of the d-Cert or the OID as specified in the "Certificate Policies" of the d-Cert concerned.

1) Format of d-Cert (Server) Certificate under root CA "HKCA Root CA 2"

For DV d-Cert (Server) issued by Sub CA "HKCA d-Cert DV SSL CA 2 - 25":-

Field Name		**Field Content**		
		HKCA DV d-Cert (Server)	**HKCA DV d-Cert (Server) with Wildcard feature**	**HKCA DV d-Cert (Server) with Multi-domain feature**
Standard fields				
Version		X.509 v3		
Serial number		[20-byte hexadecimal number set by HKCA system]		
Signature algorithm ID		sha256RSA		
Issuer name		cn=HKCA d-Cert DV SSL CA 2 - 25 o=Hong Kong Internet Registration Corporation Limited l=Hong Kong s=Hong Kong c=HK		
Validity period	**Not before**	[UTC time set by HKCA system]		
	Not after	[UTC time set by HKCA system]		
Subject name		cn=[Server Name] (Note 1) c=HK		
Subject public key info		Algorithm ID: RSA Public Key: 2048-bit key size		
Issuer unique identifier		Not used		
Subject unique identifier		Not used		
Standard extension (Note 3)				
Authority Information Access	**Certification Authority Issuer**	[URL of the Issuer's public certificate]		
	OCSP	[URL of the OCSP Responder] (Note 10)		
Authority Key Identifier		[Subject Key Identifier of the issuer's certificate]		
Key usage		Digital Signature and Key Encipherment		
		(This field will be set Critical.)		
Certificate policies (Note 12)		Policy Identifier =2.23.140.1.2.1 (Note 13) Policy Identifier = [OID] (Note 4)		
Subject alternative name	**DNS**	[Server Name in Subject name field]	[Server Name in Subject name field] + [Server Name without wildcard component] (Note 5)	[Server Name in Subject name field] + [0 to 49 Additional Server Name(s)] (Note 6)
	rfc822	Not used		
Issuer alternative name		Not used		

Basic constraints	**Subject type**	End Entity
	Path length constraint	None
		(This field will be set Critical.)
Extended key usage		Server Authentication
CRL distribution points		Distribution Point Name = [URL of CRL Distribution Point] (Note 7)
1.3.6.1.4.1.11129.2.4.2		Signed Certificate Timestamp

For OV d-Cert (Server) issued by Sub CA "HKCA d-Cert OV SSL CA 2 - 25":-

Field Name		**Field Content**		
		HKCA OV d-Cert (Server)	**HKCA OV d-Cert (Server) with Wildcard feature**	**HKCA OV d-Cert (Server) with Multi-domain feature**
Standard fields				
Version		X.509 v3		
Serial number		[20-byte hexadecimal number set by HKCA system]		
Signature algorithm ID		sha256RSA		
Issuer name		cn=HKCA d-Cert OV SSL CA 2 - 25 o=Hong Kong Internet Registration Corporation Limited l=Hong Kong s=Hong Kong c=HK		
Validity period	**Not before**	[UTC time set by HKCA system]		
	Not after	[UTC time set by HKCA system]		
Subject name		cn=[Server Name] (Note 1) o=[Subscriber Organisation Name] (Note 2) l=Hong Kong s=Hong Kong c=HK		
Subject public key info		Algorithm ID: RSA Public Key: 2048-bit key size		
Issuer unique identifier		Not used		
Subject unique identifier		Not used		
Standard extension (Note 3)				
Authority Information Access	**Certification Authority Issuer**	[URL of the Issuer's public certificate]		
	OCSP	[URL of the OCSP Responder] (Note 10)		
Authority Key Identifier		[Subject Key Identifier of the issuer's certificate]		
Key usage		Digital Signature and Key Encipherment		
		(This field will be set Critical.)		
Certificate policies (Note 12)		Policy Identifier =2.23.140.1.2.2 (Note 14) Policy Identifier = [OID] (Note 4)		
Subject alternative name	**DNS**	[Server Name in Subject name field]	[Server Name in Subject name field] + [Server Name without wildcard component] (Note 5)	[Server Name in Subject name field] + [0 to 49 Additional Server Name(s)] (Note 6)
	rfc822	Not used		
Issuer alternative name		Not used		

Basic constraints	**Subject type**	End Entity
	Path length constraint	None
		(This field will be set Critical.)
Extended key usage		Server Authentication
CRL distribution points		Distribution Point Name = [URL of CRL Distribution Point] (Note 8)
1.3.6.1.4.1.11129.2.4.2		Signed Certificate Timestamp

For EV d-Cert (Server) issued by Sub CA "HKCA d-Cert EV SSL CA 2 - 25":-

Field Name		**Field Content**
Standard fields		
Version		X.509 v3
Serial number		[20-byte hexadecimal number set by HKCA system]
Signature algorithm ID		sha256RSA
Issuer name		cn=HKCA d-Cert EV SSL CA 2 - 25 o=Hong Kong Internet Registration Corporation Limited l=Hong Kong s=Hong Kong c=HK
Validity period	**Not before**	[UTC time set by HKCA system]
	Not after	[UTC time set by HKCA system]
Subject name		cn=[Server Name] (Note 1) o=[Subscriber Organisation Name] (Note 2) Object Identifier (2.5.4.9) =[Street Address] l=Hong Kong s=Hong Kong c=HK Object Identifier (2.5.4.5) = [Subject Registration Number] Object Identifier (2.5.4.15) =[Business Category e.g. ("Private Organization"/"Government Entity"/ "Business Entity"/ "Non-Commercial Entity")] (Note 11) Object Identifier (1.3.6.1.4.1.311.60.2.1.3)=HK
Subject public key info		Algorithm ID: RSA Public Key: 2048-bit key size
Issuer unique identifier		Not used
Subject unique identifier		Not used
Standard extension (Note 3)		
Authority Information Access	**Certification Authority Issuer**	[URL of the Issuer's public certificate]
	OCSP	[URL of the OCSP Responder] (Note 10)
Authority Key Identifier		[Subject Key Identifier of the issuer's certificate]
Key usage		Digital Signature and Key Encipherment
		(This field will be set Critical.)
Certificate policies (Note 12)		Policy Identifier =2.23.140.1.1 (Note 15) Policy Identifier = [OID] (Note 4)
Subject alternative name	**DNS**	[Server Name in Subject name field] + [0 to 49 Additional Server Name(s)] (Note 6)
	rfc822	Not used
Issuer alternative name		Not used
Basic constraints	**Subject type**	End Entity

Field Name		Field Content
	Path length constraint	None
		(This field will be set Critical.)
Extended key usage		Server Authentication
CRL distribution points		Distribution Point Name = [URL of CRL Distribution Point] (Note 9)
1.3.6.1.4.1.11129.2.4.2		Signed Certificate Timestamp

Note

1. The server name (including the domain name of the server) owned by the Subscriber Organisation. In addition to English server name, Chinese server name with characters encoded in ISO/IEC 10646 is also supported. For d-Cert (Server) with Wildcard feature, the left-most component of the fully qualified domain name of the server name must be a wildcard character (i.e. an asterisk character '*', the wildcard component), meaning that the certificate may be used for all server names at the same domain or sub-domain level owned by the Subscriber Organisation (e.g. *.hkca.hk, *.subdomain.hkca.hk).

2. d-Certs are issued in English language with the organisation names in either English or Chinese language. For organisations who subscribe to d-Cert and have provided their company's Chinese name in the application form, they may determine whether to display Chinese company name on the d-Cert. If the organisation fails to provide such distinction, the company's English name shall be displayed on the d-Cert. For organisations who subscribe to d-Cert and are companies with company names in the Chinese language only or who have provided their company's Chinese name only, the company's Chinese name shall be displayed on the d-Cert (see Section 3.1.1.3 of this CPS). Moreover, the organisation branch/department name will be displayed at the same language of the company name. All standard extensions are set as "non-critical" unless otherwise specified.

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

4. 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.

5. Subject alternative name field of a d-Cert (Server) with Wildcard feature contains two server name entries. One entry is the Server Name as shown in the Subject name field that has the wildcard character (i.e. an asterisk character '*', the wildcard component) in the left-most component of the fully qualified domain name of the server name, and the other entry is the server name without the wildcard component (e.g. *.hkca.hk and hkca.hk). In addition to English server name, Chinese server name with characters encoded in ISO/IEC 10646 is also supported.

6. Subject alternative name field of a d-Cert (Server) with Multi-domain feature may contain maximum 50 server name entries. The first entry is the Server Name as shown in the Subject name field, and there may be 0 to 49 server name entries of additional server names. No wildcard character (i.e. an asterisk character '*') will be allowed as part of any server name(s). In addition to English server name, Chinese server name characters encoded in ISO/IEC 10646 is also supported.

7. URL of CRL Distribution Point for certificates issued by Sub CA "HKCA d-Cert DV SSL CA 2 - 25" is:

   http://crl.hkca.hk/crl/HKCAdCertDVSSLCA2-25CRL.crl which is a full CRL issued by the Sub CA "HKCA d-Cert DV SSL CA 2 - 25".

8. URL of CRL Distribution Point for certificates issued by Sub CA "HKCA d-Cert OV SSL CA 2 - 25" is:

   http://crl.hkca.hk/crl/HKCAdCertOVSSLCA2-25CRL.crl which is a full CRL issued by the Sub CA "HKCA d-Cert OV SSL CA 2 - 25".

9. URL of CRL Distribution Point for certificates issued by Sub CA "HKCA d-Cert EV SSL CA 2 - 25" is:

   http://crl.hkca.hk/crl/HKCAdCertEVSSLCA2-25CRL.crl which is a full CRL issued by the Sub CA "HKCA d-Cert EV SSL CA 2 - 25".

10. URL of OCSP responder is: http://ocsp.hkca.hk

11. This field contains one of the following strings: "Private Organization", "Government Entity", "Business Entity", or "Non-Commercial Entity" depending upon whether the Subscriber Organisation qualifies under the relevant terms of the CA / Browser Forum Extended Validation SSL certificate guidelines.

12. The certificate issued under this Sub CA is in compliance with this CPS and the Baseline Requirements published by CA/Browser Forum.
13. The CA/Browser Forum OID is added in this field for identification of the certificate which is issued in compliance with CA / Browser Forum Baseline Requirements – domain validated.
14. The CA/Browser Forum OID is added in this field for identification of the certificate which is issued in compliance with CA / Browser Forum Baseline Requirements – organisation identity asserted.
15. The CA/Browser Forum OID is added in this field for identification of the certificate which is issued in compliance with the CA / Browser Forum Extended Validation SSL certificate guidelines.

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

The Appendix C of this CPS provides the arrangement of updating and publishing the Certificate Revocation Lists (CRLs) issued by the Sub CAs "HKCA d-Cert DV SSL CA 2 - 25", "HKCA d-Cert OV SSL CA 2 - 25", and "HKCA d-Cert EV SSL 2 - 25", as well as the Authority Revocation List (ARL) issued by the Root CA "HKCA Root CA 2". It also specify the format of these CRLs and the ARL.

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

a) **Full CRLs** that contain Information of all revoked certificates that are issued by the Sub CAs "HKCA d-Cert DV SSL CA 2 - 25", "HKCA d-Cert OV SSL CA 2 - 25" and "HKCA d-Cert EV SSL CA 2 - 25" respectively. Each of the full CRLs is available at the following locations (URLs):

   i. Certificates issued by Sub CA "HKCA d-Cert DV SSL CA 2 - 25" :
   http://crl.hkca.hk/crl/HKCAdCertDVSSLCA2-25CRL.crl or
   ldap://ldap.hkca.hk (port 389, cn=HKCA d-Cert DV SSL CA 2 - 25 CRL, o=Hong Kong Internet Registration Corporation Limited, c=HK)

   ii. Certificates issued by Sub CA "HKCA d-Cert OV SSL CA 2 - 25" :
   http://crl.hkca.hk/crl/HKCAdCertOVSSLCA2-25CRL.crl or
   ldap://ldap.hkca.hk (port 389, cn=HKCA d-Cert OV SSL CA 2 - 25 CRL, o=Hong Kong Internet Registration Corporation Limited, c=HK)

   iii. Certificates issued by Sub CA "HKCA d-Cert EV SSL CA 2 - 25" :
   http://crl.hkca.hk/crl/HKCAdCertEVSSLCA2-25CRL.crl or
   ldap://ldap.hkca.hk (port 389, cn=HKCA d-Cert EV SSL CA 2 - 25 CRL, o=Hong Kong Internet Registration Corporation Limited, 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, HKCA shall publish the latest CRL as soon as possible after the update time. HKCA 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, HKCA may also publish supplementary update of CRLs at the HKCA web site at https://www.hkca.hk/ on ad hoc basis without prior notice.

HKCA updates and publishes the Authority Revocation List (ARL) containing information of revoked Sub CA certificates, under this CPS annually before the next update date of the respective ARL or when necessary. The latest ARL is available at the following location:

   i. Certificates issued by root CA "HKCA Root CA 2" :
   http://crl.hkca.hk/crl/HKCARootCA2ARL.crl or
   ldap://ldap.hkca.hk (port 389, cn=HKCA Root CA 2 ARL, o=Hong Kong Internet Registration Corporation Limited, c=HK)

(I) Format of Full CRL issued by the Sub CA "HKCA d-Cert DV SSL CA 2 - 25" 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=HKCA d-Cert DV SSL CA 2 - 25, o=Hong Kong Internet Registration Corporation Limited, l=Hong Kong, s=Hong Kong, c=HK	This field identifies the entity who has signed and issued the CRL.
This update		[UTC time]	"This Update" indicates the date the CRL was generated.
Next update		[UTC time]	"Next Update" contains the date by which the next CRL will be issued, but it will not be issued any later than the indicated date. Notwithstanding this, the CRL is updated and issued on a **daily** basis as stated in the CPS.
Revoked certificates	**User certificate**	[Certificate Serial Number]	Revoked certificates are listed by their serial numbers.
	Revocation date	[UTC time]	The date on which the revocation occurred is specified.
	CRL entry extensions		
	Reason code	[Revocation Reason Code]	(Note 1)
Standard extension (Note 3)			
Authority Key Identifier		[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 Full CRL issued by the Sub CA "HKCA d-Cert OV SSL CA 2 - 25" 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=HKCA d-Cert OV SSL CA 2 - 25, o=Hong Kong Internet Registration Corporation Limited, l=Hong Kong, s=Hong Kong, c=HK	This field identifies the entity who has signed and issued the CRL.
This update		[UTC time]	"This Update" indicates the date the CRL was generated.
Next update		[UTC time]	"Next Update" contains the date by which the next CRL will be issued, but it will not be issued any later than the indicated date. Notwithstanding this, the CRL is updated and issued on a **daily** basis as stated in the CPS.

Standard Fields	Sub-fields	Field Contents of Full CRL	Remarks
Revoked certificates	**User certificate**	[Certificate Serial Number]	Revoked certificates are listed by their serial numbers.
	Revocation date	[UTC time]	The date on which the revocation occurred is specified.
	CRL entry extensions		
	Reason code	[Revocation Reason Code]	(Note 1)
Standard extension (Note 3)			
Authority Key Identifier		[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.

(III) Format of Full CRL issued by the Sub CA "HKCA d-Cert EV SSL CA 2 - 25" 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=HKCA d-Cert EV SSL CA 2 - 25, o=Hong Kong Internet Registration Corporation Limited, l=Hong Kong, s=Hong Kong, c=HK	This field identifies the entity who has signed and issued the CRL.
This update		[UTC time]	"This Update" indicates the date the CRL was generated.
Next update		[UTC time]	"Next Update" contains the date by which the next CRL will be issued, but it will not be issued any later than the indicated date. Notwithstanding this, the CRL is updated and issued on a **daily** basis as stated in the CPS.
Revoked certificates	**User certificate**	[Certificate Serial Number]	Revoked certificates are listed by their serial numbers.
	Revocation date	[UTC time]	The date on which the revocation occurred is specified.
	CRL entry extensions		
	Reason code	[Revocation Reason Code]	(Note 1)
Standard extension (Note 3)			
Authority Key Identifier		[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.

(IV) Format of ARL issued by the root CA "HKCA 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.

Standard Fields	Sub-fields	Field Contents of ARL	Remarks
Signature algorithm ID		sha256RSA	This field contains the algorithm identifier for the algorithm used to sign the ARL.
Issuer name		cn=HKCA Root CA 2 o=Hong Kong Internet Registration Corporation Limited, 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)			
Authority Key Identifier		[Subject Key Identifier of the Root CA issuing this ARL]	
CRL number		[Generated by CA system]	The CRL Number is generated in sequence for each ARL issued by a CA.

Note

1. For CRL relating to d-Cert (Server), 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 at CRL entry extensions.

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

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

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

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

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

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

Root CA

Certificate subject name (CN)	**OCSP signer's certificate subject name (CN)**
"HKCA Root CA 2"	"HKCA Root CA 2 OCSP Responder"

Sub CA

Certificate subject name (CN)	**OCSP signer's certificate subject name (CN)**
"HKCA d-Cert DV SSL CA 2 - 25"	"HKCA d-Cert DV SSL CA 2 - 25 OCSP Responder"
"HKCA d-Cert OV SSL CA 2 - 25"	"HKCA d-Cert OV SSL CA 2 - 25 OCSP Responder"
"HKCA d-Cert EV SSL CA 2 - 25"	"HKCA d-Cert EV SSL CA 2 - 25 OCSP Responder"

Furthermore, a unique OID "1.3.6.1.4.1.64092.1.6" is assigned to the OCSP responders and specified in the field "Certificate Policies" of the OCSP signer's certificate. In the last section of this Appendix D, the format of OCSP response is also provided.

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

Standard Fields	**Sub-fields**	**Sub-fields**	**Field Contents**	**Remarks**
Response data	Version		v1 (0x0)	
	Responder ID	by key	[SHA-1 hash of responder's public key]	
	Produced At		[GeneralizedTime]	Time at which this response was signed (GMT+0).
	Sequence of Single Response			
	Single Response	Certificate ID	[Requested certificate identifier]	Requested certificate identifier consists of: • Hash algorithm ID • Hash of Issuer's Subject Name • Hash of Issuer's public key • Certificate serial number
		Certificate status	[Status of certificate]	Good, Revoked (with date and time (GMT+0) and revocation reason code (Note 1,2)), Unknown.
		This update	[GeneralizedTime]	Date and Time the certificate status was last known to be correct (GMT+0).
		Next update	[GeneralizedTime]	Date and Time for new updates to be made available (GMT+0).

Standard Fields	Sub-fields	Sub-fields	Field Contents	Remarks
Signature algorithm ID			sha256RSA	Algorithm that was used to sign this response.
Signature			[Signature data]	Signature of this response
Certificate			[Responder signing certificate data]	Responder's signing certificate

Note

1. For OCSP relating to d-Cert (Server), the following reason codes may be included in the field:

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

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

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

Appendix E - Summary of HKCA d-Cert Certificates by Validation Type

Features	DV d-Cert (Server) Certificates	OV d-Cert (Server) Certificates	EV d-Cert (Server) Certificates
Subscribers	Organisations that hold a valid business registration certificate issued by the Government of the Hong Kong SAR, statutory bodies of Hong Kong SAR whose existence is recognized by the laws of Hong Kong and bureaux, departments or agencies of Government of HKSAR		
Certificate Holders	Same as Subscriber		
Reliance Limit	HK$ 0	HK$ 200,000	
Recognized Certificate	Yes		
Key pair size	2048-bit RSA		
Key pair generation	Key generation by Subscriber		
Identity verification	Authentication of the identity of the domain name, and its Authorised Representative	Authentication of the identity of the domain name, the organisation, and its Authorised Representative	Authentication of the legal, physical, and operational existence of the organization, method of communication, verification of the identity of domain name, and verification of its Authorised Representative
Usage of certificate	Digital Signature, Encryption		
Subscriber's information included in the certificate	▪ Subscriber Organisation's server name and additional server names listed in the Subject Alternative Name field	▪ Subscriber Organisation's name ▪ Subscriber Organisation's server name and additional server names listed in the Subject Alternative Name field	▪ Subscriber Organisation's name, street address and business category ▪ Subscriber Organisation's server name and additional server names listed in the Subject Alternative Name field
Subscription Fees and Administration Fees	(see Section 9.1 of this CPS)		
Certificate Validity	199 days		
	(see Sections 4.6.1 and 6.3.2 of this CPS)		

Appendix F - List of Registration Authorities for the HKCA d-Cert, if any

With effect from the date of this CPS, no Registration Authority for HKCA d-Cert is appointed.

Appendix G - List of Subcontractor(s) of Certizen Limited for HKCA d-Cert Services, if any

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

Appendix H - Lifespan of CA root certificates

Reference	Name of the HKCA root certificate	Lifespan	Remarks
1	HKCA Root CA 2	20 October 2025 – 14 October 2050	
Subject DN C=HK, ST=Hong Kong, L=Hong Kong, O=Hong Kong Internet Registration Corporation Limited, CN=HKCA Root CA 2 SHA-1 Thumbprint E3:3E:C1:E1:26:FB:4F:E2:B6:1D:B7:8E:8A:EE:AD:6D:8E:BF:8E:84 SHA-256 Thumbprint 98:90:08:22:A3:D6:A9:7B:D8:31:0D:05:70:F1:E6:A5:51:B6:B8:35:6F:FE:3D:4E:82:58:23:8E:22:86:C0:6A			
2	HKCA d-Cert DV SSL CA 2 - 25	4 December 2025 – 30 November 2040	This Sub CA issues DV d-Cert (Server) from [TBC]
Subject DN C=HK, ST=Hong Kong, L=Hong Kong, O=Hong Kong Internet Registration Corporation Limited, CN=HKCA d-Cert DV SSL CA 2 - 25 SHA-1 Thumbprint 69:CA:D8:BB:F7:BB:96:CA:6E:E3:6D:68:A4:6B:B9:FF:02:E7:2B:C6 SHA-256 Thumbprint 6C:B0:1D:5B:11:20:1C:5E:5D:BD:E2:EB:0A:45:D4:00:AE:F3:FF:5E:EF:63:90:76:B9:E8:38:2D:F3:B7:92:69			
3	HKCA d-Cert OV SSL CA 2 - 25	4 December 2025 – 30 November 2040	This Sub CA issues OV d-Cert (Server) from [TBC]
Subject DN C=HK, ST=Hong Kong, L=Hong Kong, O=Hong Kong Internet Registration Corporation Limited, CN=HKCA d-Cert OV SSL CA 2 - 25 SHA-1 Thumbprint 05:40:36:DC:88:2C:12:C8:ED:1C:49:7E:B9:CB:35:93:58:8D:A0:6A SHA-256 Thumbprint C5:F4:88:39:B2:14:94:A1:16:9D:36:FB:0C:52:D1:98:FD:3F:62:DF:1D:2E:21:79:E0:94:1E:4F:B6:08:41:52			

Reference	Name of the HKCA root certificate	Lifespan	Remarks
4	HKCA d-Cert EV SSL CA 2 - 25	4 December 2025 – 30 November 2040	This Sub CA issues EV d-Cert (Server) from [TBC]
Subject DN C=HK, ST=Hong Kong, L=Hong Kong, O= Hong Kong Internet Registration Corporation Limited, CN=HKCA d-Cert EV SSL CA 2 - 25 SHA-1 Thumbprint 4F:CE:70:57:A4:DC:45:07:A6:3A:01:26:E8:73:17:90:51:B8:23:5D SHA-256 Thumbprint 97:7B:CE:D8:9D:7B:83:75:1D:65:0E:C3:B6:FD:94:72:B7:13:B2:3B:8E:C1:FC:EC:0F:96:6D:53:67:7E:44:5E			

THIS IS THE LAST PAGE OF
CERTIFICATION PRACTICE STATEMENT