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 (Personal)
HKCA d-Cert (Organisational)
HKCA d-Cert (Encipherment)

Date : [TBC]
OID : 1.3.6.1.4.1.64092.1.1.1

Table of Contents

PREAMBLE 5
1. INTRODUCTION 7
1.1 Overview 7
1.2 Community and Applicability 7
1.2.1 Certification Authority 7
1.2.2 End Entities 8
1.2.3 Classes of Subscribers 9
1.2.4 Certificate Lifespan 10
1.2.5 Official Website and d-Cert Subscriber Portal 10
1.3 Contact Details 10
1.4 Complaints Handling Procedures 11
2. GENERAL PROVISIONS 12
2.1 Obligations 12
2.1.1 CA Obligations 12
2.1.2 RA Obligations and Liability 12
2.1.3 Contractor Obligations 12
2.1.4 Subscriber Obligations 13
2.1.5 Subscriber's Liability 14
2.1.6 Relying Party's Obligations 14
2.2 Further Provisions 14
2.2.1 Reasonable Skill and Care 14
2.2.2 No Supply of Goods 15
2.2.3 Limitation of Liability 16
2.2.4 HKCA's Liability for Received but Defective Certificates 18
2.2.5 Assignment by Subscriber 19
2.2.6 Authority to Make Representations 19
2.2.7 Variation 19
2.2.8 Retention of Title 19
2.2.9 Conflict of Provisions 19
2.2.10 Fiduciary Relationships 19
2.2.11 Cross Certification 19
2.2.12 Concerning the Comparison of the Scope of Contents of this CPS with the RFC3647 Standard 19
2.2.13 Financial Responsibility 19
2.3 Interpretation and Enforcement (Governing Law) 19
2.3.1 Governing Law 20
2.3.2 Severability, Survival, Merger, and Notice 20
2.3.3 Dispute Resolution Procedures 20
2.3.4 Interpretation 20
2.4 Subscription Fees 20
2.5 Publication and Repository 20
2.5.1 Certificate Repository Controls 21
2.5.2 Certificate Repository Access Requirements 21
2.5.3 Certificate Repository Update Cycle 21
2.5.4 Permitted Use of Information Contained in the Repository 21
2.6 Compliance Assessment 21
2.7 Confidentiality 21
3. IDENTIFICATION AND AUTHENTICATION 22
3.1 Initial Application 22
3.1.1 Types of Names 23
3.1.2 Need for Names to be Meaningful 24
3.1.3 Rules for Interpreting Various Names 24
3.1.4 Name Uniqueness 24
3.1.5 Name Claim Dispute Resolution Procedure 24
3.1.6 Infringement and Violation of Trademarks 24

3.1.7 Method to Prove Possession of the Private Key 24
3.1.8 Authentication of Identity of Organisational Applicant 25
3.1.9 Authentication of Identity of Personal Applicant 26
3.2 Certificate Renewal 27
3.2.1 Renewal of d-Cert (Personal) Certificates 27
3.2.2 Renewal of d-Cert (Organisational), and d-Cert (Encipherment) Certificates 28
4. OPERATIONAL REQUIREMENTS 30
4.1 d-Cert (Personal) Certificates 30
4.1.1 Certificate Application 30
4.1.2 Certificate Issuance 30
4.1.3 Publication of d-Cert 32
4.2 d-Cert (Organisational) Certificates 32
4.2.1 Certificate Application 32
4.2.2 Certificate Issuance 32
4.2.3 Publication of d-Cert 34
4.3 d-Cert (Encipherment) Certificates 34
4.3.1 Certificate Application 34
4.3.2 Certificate Issuance 35
4.3.3 Publication of d-Cert 36
4.4 Timeframe for Processing Certificate Applications 36
4.5 Certificate Suspension and Revocation 36
4.5.1 Circumstances for Suspension and Revocation 36
4.5.2 Revocation Request Procedure 38
4.5.3 Service Pledge & Update of Certificate Revocation List 38
4.5.4 Effect of Revocation 40
4.6 Termination of Certificate Subscription 40
4.7 Computer Security Audit Procedures 40
4.7.1 Types of Events Recorded 40
4.7.2 Frequency of Processing Log 40
4.7.3 Retention Period for Audit Logs 40
4.7.4 Protection of Audit Logs 41
4.7.5 Audit Log Backup Procedures 41
4.7.6 Audit Information Collection System 41
4.7.7 Notification of Event-Causing Subject to HKCA 41
4.7.8 Vulnerability Assessments 41
4.8 Records Archival 41
4.8.1 Types of Records Archived 41
4.8.2 Archive Retention Period 41
4.8.3 Archive Protection 42
4.8.4 Archive Backup Procedures 42
4.8.5 Timestamping 42
4.9 Key Changeover 42
4.10 Disaster Recovery and Key Compromise Plans 42
4.10.1 Disaster Recovery Plan 42
4.10.2 Key Compromise Plan 43
4.10.3 Key Replacement 43
4.10.4 Damaged Computing Resources, Software and/or Data 43
4.11 CA Termination 43
4.12 RA Termination 43
5. PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY CONTROLS 44
5.1 Physical Security 44
5.1.1 Site Location and Construction 44
5.1.2 Access Controls 44
5.1.3 Environmental controls of Computer Cabinet 44
5.1.4 Power and Air Conditioning 45
5.1.5 Natural Disasters 45
5.1.6 Fire and Flooding Prevention and Protection 45

5.1.7 Media Storage 45
5.1.8 Off-site Backup 45
5.1.9 Custody of Subscriber Agreements and Other Documents 45
5.1.10 Waste Disposal Procedures 45
5.2 Procedural Controls 45
5.2.1 Trusted Role 45
5.2.2 Transfer of Document and Data between HKCA, Contractor and RAs 46
5.2.3 Annual Assessment 46
5.3 Personnel Controls 46
5.3.1 Background and Qualifications 46
5.3.2 Background Investigation 46
5.3.3 Training Requirements 46
5.3.4 Assessment of Existing Staff 46
5.3.5 Documentation Supplied To Personnel 46
6. TECHNICAL SECURITY CONTROLS 47
6.1 Key Pair Generation and Installation 47
6.1.1 Key Pair Generation 47
6.1.2 Subscriber Private Key Delivery 47
6.1.3 Public Key Delivery to Subscriber 47
6.1.4 Key Sizes 47
6.1.5 Standards for Cryptographic Module 47
6.1.6 Key Usage Purposes 47
6.2 Private Key Protection 47
6.2.1 Standards for Cryptographic Module 48
6.2.2 Private Key Multi-Person Control 48
6.2.3 Private Key Escrow 48
6.2.4 Backup of HKCA Private Keys 48
6.2.5 Private Key Transfer between Cryptographic Modules 48
6.3 Other Aspects of Key Pair Management 48
6.4 Computer Security Controls 48
6.5 Life Cycle Technical Security Controls 48
6.6 Network Security Controls 49
6.7 Cryptographic Module Engineering Controls 49
7. CERTIFICATE PROFILE, CERTIFICATE REVOCATION LIST 50
7.1 Certificate Profile 50
7.2 Certificate Revocation List Profile 50
8. CPS ADMINISTRATION 51
Appendix A - Glossary 52
Appendix B - HKCA d-Cert Format 57
Appendix C - HKCA Certificate Revocation Lists (CRLs) and Authority Revocation List (ARL) Format 65
Appendix D - Summary of HKCA d-Cert Features 69
Appendix E - List of Registration Authorities for the HKCA d-Cert 72
Appendix F - List of Subcontractor(s) of Certizen Limited for HKCA d-Cert Services, if any 73
Appendix G - Lifespan of CA root certificates 74
Appendix H – List of Particular Applications and Corresponding Application-specific Codes for HKCA d-Cert 75
Appendix I - Table of Comparison of Request for Comments (“RFC”) 3647 and this CPS 76

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 ("Recognized 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 F**. Certizen Limited, together with its Subcontractor(s) under the Contract, if any, is hereafter referred to as the "Contractor" for the purpose of this CPS.

For the purposes of this document, the Hong Kong Internet Registration Corporation Limited is referred to as HKIRC or 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 E**.

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 or suspension, and publication in a publicly available Repository of recognized and accepted digital certificates for secure online identification. The d-Cert (Personal), d-Cert (Organisational), and d-Cert (Encipherment) certificates issued under this CPS 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, and the structure of this CPS is as follows:

Section 1	provides an overview and contact details
Section 2	sets out the responsibilities and liabilities of the parties
Section 3	sets out application and identity confirmation procedures
Section 4	describes the operational requirements
Section 5	presents the security controls
Section 6	sets out how the Public/Private Key pairs will be generated and controlled
Section 7	describes the certificate, certificate revocation list and online certificate status protocol response profiles
Section 8	documents how this CPS will be administered
Appendix A	contains a glossary
Appendix B	contains formats of d-Certs issued under this CPS
Appendix C	contains formats of HKCA Certificate Revocation List (CRL), Authority Revocation List (ARL)
Appendix D	contains a summary of features of d-Certs issued under this CPS
Appendix E	contains a list of HKCA d-Cert Registration Authorities (RAs), if any
Appendix F	contains a list of Subcontractor(s) of Certizen Limited for HKCA d-Cert Services, if any
Appendix G	describes lifespan of CA root certificates
Appendix H	contains a list of particular applications and corresponding application-specific codes for HKCA d-Cert
Appendix I	contains a table of comparison of RFC3647 and this CPS

1. INTRODUCTION

1.1 Overview

This Certification Practice Statement ("CPS") is published for public knowledge by 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 or suspending and publishing certificates.

HKCA will 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**") **"1.3.6.1.4.1.64092.1.1.1"** (see description of the field "Certificate Policies" in **Appendix B**).

This CPS sets out the roles, functions, obligations, and potential liabilities of the participants in the system used by 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 (Personal), d-Cert (Organisational) and d-Cert (Encipherment) 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 or suspension, and publication in a publicly available Repository of accepted Recognized Certificates. Recognized Certificates have characteristics of accuracy and contain representations of fact which are defined in law by the Ordinance, including a representation (as further defined below) that such certificates have been issued in accordance with this CPS. The appointment of agents by HKCA does not diminish HKCA's obligation to use a Trustworthy System, nor does it alter the characteristics of d-Certs as Recognized Certificates.

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

1.2 Community and Applicability

1.2.1 Certification Authority

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

1.2.1.1 Representations by HKCA

By issuing a certificate that refers to this CPS, HKCA represents to Relying Parties who act in accordance with Section 2.1.6 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 2.1.6 and other

relevant sections of this CPS, that HKCA has issued the certificate to the Subscriber identified in it.

1.2.1.2 Effect

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

1.2.1.3 HKCA's Right to Subcontract

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 will remain liable for the performance of the CPS and the Subscriber Agreement as if such sub-contracting had not occurred.

1.2.2 End Entities

Under this CPS there are two types of end entities, Subscribers and Relying Parties. A Subscriber is the "Subscriber" or "Subscriber Organisation" referred to in **Appendix A**. Relying Parties are entities that have relied on any class or category of certificate issued by 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 RAs or the Contractor. For d-Certs that are issued via the RAs 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 issuance of those d-Certs (see also Sections 2.1.2 and 2.1.3). Subscribers who rely on a d-Cert of another Subscriber in a transaction will be Relying Parties in respect of such a certificate. **NOTE TO RELYING PARTIES: Unless otherwise specified, the HKCA's d-Cert system is not age restricted and minors may apply for and receive d-Certs.**

1.2.2.1 Warranties and Representations by Applicants and Subscribers

Each Applicant (represented by an Authorised Representative in the case of applying for a d-Cert (Organisational) or d-Cert (Encipherment) certificate) must accept the terms specified in this CPS. This acceptance includes a commitment from the Applicant that, by accepting a certificate issued under this CPS, the Applicant warrants (promises) to HKCA and represents to all other relevant parties, particularly Relying Parties, that the following facts are and will remain true throughout the certificate's operational period:

a) No person other than the Subscriber of a d-Cert (Personal), the Authorised User of a d-Cert (Organisational) certificate or the Authorised Unit of a d-Cert (Encipherment) certificate has had access to the Subscriber's Private Key.
b) Each Digital Signature generated using the Subscriber's Private Key, which corresponds to the Public Key contained in the Subscriber's d-Cert, is the Digital Signature of the Subscriber.
c) A d-Cert (Encipherment) certificate is to be used only for the purposes stipulated in Section 1.2.3.3 below.
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.

1.2.3 Classes of Subscribers

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

1.2.3.1 d-Cert (Personal) Certificates

A d-Cert (Personal) certificate is issued under this CPS and the Subscriber Agreement to individuals who have a HKID Card. These certificates may be used to perform commercial operations.

A d-Cert (Personal) certificate may be issued to persons aged under 18 who have a HKID Card (see also Section 3.1.1.2).

1.2.3.2 d-Cert (Organisational) Certificates

A d-Cert (Organisational) certificate is issued to (i) Bureaux and Departments of the Government of Hong Kong SAR, (ii) organisations that hold a valid business registration certificate issued by the Government of the Hong Kong SAR or a valid certification letter issued by the Inland Revenue Department of the Government of the Hong Kong SAR to the Reporting Financial Institution / Reporting Entity as referred in the Inland Revenue Ordinance (Cap. 112), and (iii) statutory bodies of Hong Kong whose existence is recognized by the laws of Hong Kong SAR (collectively referred to as the "Subscriber Organisation"); and identifies a member or employee whom that Subscriber Organisation has duly authorised to use the Private Key of that d-Cert (Organisational) (the "Authorised User"). These certificates may be used for the same purposes as d-Cert (Personal) certificates.

Subscriber Organisations, including but not limited to Reporting Financial Institutions and Reporting Entities as referred in the Inland Revenue Ordinance (Cap. 112) that hold a valid certification letter issued by the Inland Revenue Department of the Government of Hong Kong SAR, undertake to HKCA not to give authority to the authorized user of the d-Cert (Organisational) to use the certificate for any purpose other than to encrypt and decrypt electronic messages, or to generate a digital signature within the particular application referred to in Appendix H.

1.2.3.3 d-Cert (Encipherment) Certificates

A d-Cert (Encipherment) certificate is issued to (i) Bureaux and Departments of the Government of Hong Kong SAR, (ii) organisations that hold a valid business registration certificate issued by the Government of Hong Kong SAR and (iii) statutory bodies of Hong Kong SAR whose existence is recognized by the laws of Hong Kong SAR (collectively referred to as the "Subscriber Organisation"). Such a certificate is designed for use by a unit of the Subscriber Organisation which has been duly authorised by the Subscriber Organisation to use the Private Key of that d-Cert (Encipherment) certificate (the "Authorised Unit").

Certificates of this class are to be used only:

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

Subscriber Organisations undertake to HKCA not to give authority to the Authorised Unit to use a Digital Signature of this class of certificate for any other purpose. Accordingly, any digital signature generated by the private key of this class of certificate used other than to acknowledge receipt of a message as set out above must be regarded as

a signature generated and used without the authority of the Subscriber Organisation whose signature it is, and must be treated as an unauthorised signature for all purposes.

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

1.2.4 Certificate Lifespan

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

When applying for a d-Cert, the applicant will choose the validity period. The available validity periods for certificates issued under this CPS to new Applicants are as follows:

Certificate type	Validity period specified in the certificate
d-Cert (Personal)	1 year, 2 years or 3 years
d-Cert (Organisational)	1 year or 2 years
d-Cert (Encipherment)	1 year, 2 years or 3 years

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

1.2.5 Official Website and d-Cert Subscriber Portal

HKCA offers d-Cert services through its official website and subscriber portal at the following URLs:

CA website: https://www.hkca.hk
d-Cert Subscriber Portal: https://www.hkca.hk/subscriber

All first-time applications and applications for a d-Cert following the revocation or expiration of a d-Cert are considered new applications. These applications must be submitted through the d-Cert Subscriber Portal, where the Applicant must have successfully authenticated using "iAM Smart+".

The online application process will comply with the procedures described in Sections 3 and 4 of this CPS.

1.3 Contact Details

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

1.4 Complaints Handling Procedures

HKCA will 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 will contact the complainants by phone, email or letter mail to acknowledge and reply to the complaints.

2. GENERAL PROVISIONS

2.1 Obligations

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, suspending, revoking and publishing certificates in conformity with the Ordinance and this CPS, and places a monetary limit in respect of such liability as it may have as set out below and in the certificates issued.

2.1.1 CA Obligations

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

a) issue and publish certificates in a timely manner (see Section 2.5);
b) notify Applicants of the approval or rejection of their applications (see Sections 4.1 to 4.3);
c) suspend or revoke certificates and publish Certificate Revocation Lists in a timely manner (see Section 4.5); and
d) notify Subscribers of the suspension or revocation of their certificates (see Sections 4.5.1, 4.5.2 and 4.5.3).

2.1.2 RA Obligations and Liability

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 will not become parties to any Subscriber Agreement, nor will they accept any duty of care to Subscribers or Relying Parties, in connection with the issuance, revocation or suspension 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 will 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.**

2.1.3 Contractor Obligations

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.

2.1.4 Subscriber Obligations

Subscribers are responsible for:

a) Agreeing that the key pair is generated by HKCA in a Trustworthy System and environment within HKCA's designated premises on behalf of the Subscriber when applying for a d-Cert (Personal), d-Cert (Organisational), or d-Cert (Encipherment) certificate.

b) Properly completing the application procedures and confirming acceptance of the Subscriber Agreement (by the Authorised Representative in the case of applying for a d-Cert (Organisational) certificate, or d-Cert (Encipherment) certificate) in the appropriate form, including digital signing via "iAM Smart+", as well as fulfilling the obligations placed upon them by that Agreement, while ensuring the accuracy of representations in certificate application.

c) Acknowledging that the d-Cert certificate, Private Key, and d-Cert PIN are delivered through secured electronic methods:
   i) The Private Key and the corresponding d-Cert certificate can be downloaded from the d-Cert Subscriber Portal using the registered account of the Subscriber. For d-Cert (Organisational) or d-Cert (Encipherment), the download is available through the Authorised Representative's registered account.
   ii) The d-Cert PIN is distributed separately via secure, one-time-use download links. These links are sent to the registered email of the Subscriber. For d-Cert (Organisational), the link is sent to the Authorised User's registered email, and for d-Cert (Encipherment), to the Authorised Unit's registered email.

d) Securely managing these electronic credentials and ensuring the confidentiality of download links and PIN access.

e) Accurately following the procedures specified in this CPS regarding the expiry of certificates.

f) Acknowledging their obligation to protect the confidentiality (i.e. keep it secret) and integrity of their Private Key using reasonable precautions to prevent loss, disclosure, or unauthorised use, and accepting responsibility for any consequences under any circumstances for the compromise of the Private Key.

g) Immediately reporting to HKCA upon discovering the loss or compromise of their Private Key (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).

h) Notifying HKCA immediately of any change in the Information in the certificate provided by the Subscriber or of any change in the Authorised User.

i) Informing HKCA immediately about any changes regarding the appointment or information of the Authorised Representative for d-Cert (Organisational), d-Cert (Encipherment).

j) Reporting any loss, compromise, or unauthorized use of Private Keys or received PIN codes to HKCA immediately, to permit prompt revocation or other remedial actions.

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

l) Agreeing that by having been issued or accepting a certificate they warrant (promise) to HKCA and represent to all Relying Parties that during the operational period of the certificate, the facts stated in Section 1.2.2.1 above are and will remain true.

m) Not using a certificate in a transaction on becoming aware of any ground upon which HKCA could suspend or 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 suspend or revoke the certificate under the terms of this CPS.

n) Upon becoming so aware of any ground upon which HKCA could suspend or revoke the certificate, or upon the Subscriber making a revocation request or upon being notified by

HKCA of its intention to suspend or revoke the certificate, immediately notifying Relying Parties in any transaction that remains to be completed at the time, that the certificate used in that transaction is liable to be suspended or revoked (either by 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.

o) Acknowledging that by submitting a d-Cert online application via the d-Cert Subscriber Portal, they authorise the publication of the d-Cert to any other person or in the HKCA's Repository.

p) For the purpose of identity authentication, using the Private Key of a d-Cert only during its validity period.

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

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

2.1.5 Subscriber's Liability

Each Subscriber acknowledges that if they do not discharge their responsibilities as set out above properly or at all, each Subscriber may become liable under the Subscriber Agreement and/or in law to pay 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.

2.1.6 Relying Party's Obligations

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

a) Relying on such certificates only when the reliance is reasonable and in good faith in light of all the circumstances known to the Relying Party at the time of the reliance.

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

c) Checking the status of the certificate on the certificate revocation list 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.

2.2 Further Provisions

Obligations of HKCA to Subscribers and Relying Parties

2.2.1 Reasonable Skill and Care

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 the 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 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 if HKCA, the Contractor or the RA acting on HKCA's behalf has exercised a reasonable degree of skill and care, they 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, if HKCA (by 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 HKCA, the Contractor, nor any such RA will be 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.

2.2.2 No Supply of Goods

For the avoidance of doubt, a Subscriber Agreement is not a contract for the supply of goods of any description or at all. Any and all certificates issued pursuant to it remain the property of and in the possession and control of 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 will exercise reasonable care to see that the same is fit for the purposes of completing and accepting a certificate as set out in this CPS, and if it is not, then HKCA's liability will be as set out in sections 2.2.3 - 2.2.4 below. 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.

2.2.3 Limitation of Liability

2.2.3.1 Reasonableness of Limitations

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

2.2.3.2 Limitation on Types of Recoverable Loss

In the event of 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 will 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.

2.2.3.3 Liability Limit of HK$ 200,000

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 will not under any circumstances exceed, HK$200,000 in respect of one d-Cert, or HK$0 (zero) in respect of one d-Cert (Personal) certificate issued to a person under 18, regardless of the number of transactions involved in that one d-Cert certificate.

2.2.3.4 Time Limit For Making Claims

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, suspension, 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 will be waived and absolutely barred.

2.2.3.5 HKCA, the Contractor, RAs and their Personnel

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 Subscribers 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 Subscribers 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.

2.2.3.6 Liability For Wilful Misconduct, Personal Injury or Death

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

2.2.3.7 Certificate Notices, Limitations and Reliance Limit

Certificates issued by HKCA will 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 website 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 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 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, or HK$0 if this certificate is a d-Cert (Personal) certificate issued to a person under 18, in respect of proved loss caused by reasonable reliance upon such inaccurate or misleading matters in this certificate where such losses are not and do not include (1) any direct or indirect loss of profits or revenue, loss or injury to reputation or goodwill, loss of any opportunity or chance, loss of projects, or the loss or loss of use of any data, equipment or software or (2) any indirect, consequential or incidental loss or damage even if, in respect of the latter, 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 d-Cert (Personal) certificate issued to a person under 18, and in all cases in relation to categories of loss (1) and (2), is HK$0.

None of the 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, suspension, 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 will 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."

2.2.4 HKCA's Liability for Received but Defective Certificates

Notwithstanding the limitation of HKCA's liability set out above, if, after receiving the certificate, a Subscriber finds that, because of any error in the Private Key or Public Key of the certificate, no transactions contemplated by the PKI can be completed properly or at all, and that Subscriber notifies HKCA of this immediately to permit the certificate to be revoked and (if desired) re-issued, then, if such notification has occurred within 3 months after receiving the certificate and the Subscriber no longer wants a certificate, HKCA, on being satisfied of the existence of any such error will refund the fee paid. If the Subscriber waits longer than 3 months

after receiving the certificate before notifying HKCA of any such error, the fee paid will not be refunded as of right, but only at the discretion of HKCA.

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

2.2.6 Authority to Make Representations
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.

2.2.7 Variation
HKCA has the right to vary this CPS without notice (See Section 8). The 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.

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

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

2.2.10 Fiduciary Relationships
None of 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.

2.2.11 Cross Certification
In all instances in relation to the d-Cert (Personal), d-Cert (Organisational), d-Cert (Encipherment) issued under this CPS, HKCA reserves the right to define and determine suitable grounds for cross-certification with another CA.

2.2.12 Concerning the Comparison of the Scope of Contents of this CPS with the RFC3647 Standard
This CPS has been prepared with reference to the Request for Comments ("RFC") 2527 standard. As the current format has long been adopted and understood by Subscribers and Relying Parties, and other relevant parties, a substantial structural change to conform to RFC 3647 standard may cause confusion. Accordingly, a comparison table aligning the RFC 3647 CPS structure with the corresponding sections of this CPS is provided in **Appendix I** for reference.

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

2.3 Interpretation and Enforcement (Governing Law)

2.3.1 Governing Law

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

2.3.2 Severability, Survival, Merger, and Notice

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

2.3.3 Dispute Resolution Procedures

The decisions of 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

2.3.4 Interpretation

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

2.4 Subscription 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)).

2.5 Publication and Repository

Under the Ordinance, HKCA maintains a Repository that contains a list of accepted certificates issued under this CPS, the current certificate revocation list, the HKCA Public Key, a copy of this CPS, and other Information related to d-Cert certificates referencing this CPS, such as the "Subscribers Terms and Conditions" available on the CA website and d-Cert Subscriber Portal. This CPS and the latest version of "Subscribers Terms and Conditions" will constitute the public Subscriber Agreement and Relying Party Agreement. HKCA will promptly publish and update the Repository regarding the relevant disclosed documents and disclosure records of the previously published documents and their amendments. The Repository is available on a substantially 24 hours per day, 7 days per week basis, subject to scheduled maintenance of an average of 2 hours per week and any emergency maintenance. HKCA promptly publishes each certificate accepted by and issued to the Subscriber under this CPS in the Repository. The Repository can be accessed at URLs as follows:

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

2.5.1 Certificate Repository Controls

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

2.5.2 Certificate Repository Access Requirements

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

2.5.3 Certificate Repository Update Cycle

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

2.5.4 Permitted Use of Information Contained in the Repository

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

2.6 Compliance Assessment

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

2.7 Confidentiality

HKCA will 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, suspending, revoking and publishing d-Certs will not disclose or permit or suffer to be disclosed any information relating to another person as contained in such record, book, register, correspondence, information, document or other material to any other person. Information about Subscribers that is submitted as part of an application for a d-Cert 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. 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.

3. IDENTIFICATION AND AUTHENTICATION

HKCA is responsible for establishing the requirements for verifying new and renewal applications for d-Cert, as well as subsequent revocation requests. HKCA reserves its absolute right to approve or reject any new or renewal application for d-Cert, as well as revocation requests, without providing explanations or reasons.

3.1 Initial Application

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**).

HKCA undertakes the necessary procedures to verify the details received from the d-Cert applications:

- For d-Cert (Personal) certificate applications: the identity of the Applicant;
- For d-Cert (Organisational) certificate applications: the identity of the Applicant, the Authorised Representative, and each Authorised User, as well as the validity of the Authorised Representative's authorisation from the Applicant;
- For d-Cert (Organisational) with AEOI Function certificate applications: the identity of the Applicant, the Authorised Representative, and each Authorised User, as well as the validity of the Authorised Representative's authorisation from the Applicant and each Authorised User;
- For d-Cert (Encipherment) certificate applications: the identity of the Applicant and the Authorised Representative, as well as the validity of the Authorised Representative's authorisation from the Applicant.

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

- For d-Cert (Personal) certificate:
  a) The Applicant has created a personal 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 Applicant has digitally signed the certificate application using "iAM Smart+".
- For d-Cert (Organisational) and d-Cert (Encipherment) certificate:
  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 provided through "iAM Smart+" as sufficient proof of identity. Identity authentication of the Authorised Users named in d-Cert (Organisational) certificates is not required. Once the application is approved, HKCA will prepare the d-Cert and notify the Applicant of the issuance process.

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.

3.1.1 Types of Names

3.1.1.1 d-Cert (Personal) certificates

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

3.1.1.2 d-Cert (Personal) certificates issued to Subscribers who are under 18

For a d-Cert (Personal) certificate, the Subscriber is identified in the certificate with a Subject Name specified in Section 3.1.1.1 and the wording "d-Cert (Personal/Minor)" (see **Appendix B**) to indicate that the Subscriber is under 18 at the time the certificate is issued.

3.1.1.3 d-Cert (Organisational) certificates

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

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

3.1.1.4 d-Cert (Encipherment) certificates

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

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

3.1.1.5 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 (Organisational) certificate, or d-Cert (Encipherment) certificate, that person will not be identified in the d-Cert.

3.1.1.6 Organisation Names in Chinese Language

d-Cert (Personal) certificates are issued in English language only.

d-Cert (Organisational) certificates are issued in English language. However, if the organisation's name and branch name in Chinese are provided in the application, these will also be included on the certificate. For Organisations whose registered company name exists only in the Chinese language, the default English name will be set as "***CHINESE NAME ONLY***".

d-Cert (Encipherment) certificates are issued in English language only. If an Organisation subscribing to a d-Cert (Encipherment) certificate has provided only its Chinese company name, or if its registered company name exists only in Chinese, the company name will not be displayed on the d-Cert.

3.1.2 Need for Names to be Meaningful

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

3.1.3 Rules for Interpreting Various Names

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

3.1.4 Name Uniqueness

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

3.1.5 Name Claim Dispute Resolution Procedure

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

3.1.6 Infringement and Violation 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, trade name, company name, or any other intellectual property rights of any third party.

3.1.7 Method to Prove Possession of the Private Key

HKCA will carry out central key generation services on behalf of the Subscriber within a Trustworthy System and environment at HKCA's designated premises, for the purpose of safeguarding the security and integrity of the Private Key.

The Private Key, together with the corresponding certificate, will be delivered to the Subscriber exclusively through secure online channels. Upon successful issuance, HKCA will dispatch two (2) separate electronic communications to the Subscriber, as set out below:

- For d-Cert (Personal) certificate
  - a) a notification enabling the Subscriber to download the certificate and Private Key, packaged in PKCS#12 format file, through the Subscriber's duly registered personal account; and
  - b) a secure electronic link for retrieval of the PIN. Such link will be valid for one (1) use only and will automatically expire one (1) calendar month from the date of issuance.
- For d-Cert (Organisational) certificate
  - a) a notification enabling the Subscriber to download the certificate and Private

Key, each packaged in PKCS#12 format, through the Subscriber's duly registered corporate account; and

b) a secure electronic link transmitted to each Authorized User's designated email address for retrieval of such Authorized User's 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.

- For d-Cert (Encipherment) certificate
  a) a notification enabling the Subscriber to download the certificate and Private Key, each packaged in PKCS#12 format, through the Subscriber's duly registered corporate account; and
  b) a secure link transmitted to each Authorized Unit's designated email address for retrieval of such Authorised Unit's 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.

Upon the Subscriber's successful completion of (a) the download of the certificate and Private Key and (b) the retrieval of the associated PIN, HKCA will forthwith and permanently delete the Private Key and the PIN from its systems. This process will constitute conclusive proof of possession of the Private Key in a secure and auditable manner, in accordance with Sections 4.1, 4.2, and 4.3 herein.

3.1.8 Authentication of Identity of Organisational Applicant

3.1.8.1 Confirmation of the identity of an Organisational Applicant of d-Cert (Organisational) and d-Cert (Encipherment) certificates 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) The Applicant's Authorised Representative will appear at a HKCA's designated premises, or premises of the Contractor or RA designated by HKCA, to submit a duly completed and signed d-Cert application form together with the Subscriber Agreement, and to present his or her HKID Card or passport for identity verification. Personnel at the aforementioned premises will conduct face-to-face verification of the Authorised Representative's identity, review and certify the application package, and thereafter transmit the application to the HKCA processing centre for further processing.

c) 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.

d) 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.

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

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

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

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

3.1.8.4 Applications from Bureaux or Departments of the Government of Hong Kong SAR must be accompanied by a copy of a memo, a letter, or a relevant application form impressed with the relevant Bureau or Department chop, appointing the Authorised Representative to act on behalf of the Bureau or Department in matters 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.

3.1.8.5 For Subscriber Organisations that have been issued a d-Cert (Organisational) or d-Cert (Encipherment) certificate with a validity period exceeding one year, HKCA will re-verify the continued legal existence of the Subscriber Organisation, approximately at the end of each anniversary of the certificate during its validity period. HKCA may suspend or revoke the certificates issued to that Subscriber Organisation in accordance with Section 4.5 (Certificate Suspension and Revocation) of this CPS if the existence of the Subscriber Organisation cannot be attested.

3.1.9 Authentication of Identity of Personal Applicant

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

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

b) The Applicant will appear at a HKCA's designated premises, or premises of the Contractor or RA designated by HKCA, to submit a duly completed and signed d-Cert application form together with the Subscriber Agreement, and to present his or her HKID Card or passport for identity verification. Personnel at the aforementioned premises will conduct face to face verification of the Applicant's identity, review and certify the application package, and thereafter transmit the application to the HKCA processing centre for further processing.

c) The Applicant will present his valid Digital Signature supported by a valid d-Cert (Personal) certificate.

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

3.2 Certificate Renewal

All d-Cert Subscribers must submit renewal applications for their d-Cert either through the d-Cert Subscriber Portal, or through the Contractor or a RA, where applicable (see **Appendix E**). Renewal applications must be submitted sufficiently in advance of the certificate expiry date, and in any event no later than the deadline prescribed by HKCA, in order to avoid interruption of certificate validity and associated services.

3.2.1 Renewal of d-Cert (Personal) Certificates

3.2.1.1 HKCA will notify Subscribers to renew their d-Cert (Personal) certificates prior to the expiry of the certificates' validity period. Renewal applications will be submitted through the d-Cert Subscriber Portal. The certificates may be renewed before expiry of their validity at the request of the Subscriber and at the discretion of HKCA. Identity authentication for renewal applications will be performed through digital signature via "iAM Smart+". HKCA will not perform renewal of expired, suspended, or revoked certificates. At the discretion of HKCA, the validity period of the new certificate issued to the Subscriber may be longer than the validity period specified in Section 1.2.4.:

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

Three years	The date the new certificate is generated	The date that is three years after the expiry date of the old certificate being renewed	The new certificate may have a validity period of more than three years but no more than three years and one month

Note: 1. See Section 1.2.4.

3.2.1.2 There is no automatic certificate renewal of a d-Cert (Personal) certificate. The process of "Authentication of Identity of Personal Applicant" described in Section 3.1.9 will normally apply. However, a d-Cert (Personal) certificate may be renewed without the Subscriber's personal attendance, provided that the renewal application is submitted through the d-Cert Subscriber Portal and is digitally signed by the Applicant using "iAM Smart+" as specified in Section 3.1.9(a), or with a valid digital signature as specified in Section 3.1.9(c). In all other cases, the Subscriber is required to submit a duly completed and signed certificate renewal form to HKCA to apply for renewal. Details of the renewal application process are available on the HKCA website.

3.2.1.3 Upon renewal, a new key pair will be generated through HKCA's central key generation service. The terms and conditions of the original Subscriber Agreement will remain applicable to the renewed certificate, except where such terms are inconsistent with the terms of the current CPS in effect on the date of renewal, in which case the current CPS will prevail. Subscribers intending renewal are advised to review the CPS in effect at the time of renewal prior to submitting their renewal applications.

3.2.2 Renewal of d-Cert (Organisational), and d-Cert (Encipherment) Certificates

3.2.2.1 HKCA will notify Subscribers to renew their d-Cert (Organisational) and d-Cert (Encipherment) certificates prior to the expiry of the certificates' validity period. The certificates may be renewed before expiry of their validity at the request of the Subscriber and at the discretion of HKCA. HKCA will not perform renewal of expired, suspended, or revoked certificates. At the discretion of HKCA, the validity period of the new certificate issued to the Subscriber may be longer than the validity period specified in Section 1.2.4.

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

Note: 1. See Section 1.2.4.
2. For d-Cert (Encipherment) only

3.2.2.2 There is no automatic certificate renewal of a d-Cert (Organisational) or d-Cert (Encipherment) certificates. However, a d-Cert (Organisational) or d-Cert (Encipherment) certificate may be renewed without the Authorised Representative's personal attendance, provided that the renewal application is submitted through the d-Cert Subscriber Portal and is digitally signed by the Authorised Representative using "iAM Smart+" as specified in Section 3.1.8.1(a), or with a valid digital signature as specified in Section 3.1.8.1(c). In all other cases, the Authorised Representative is required to submit a duly completed and signed certificate renewal form to HKCA to apply for renewal. Details of the renewal application process are available on the HKCA website. In circumstances where Authorised Representatives are replaced, the new Authorised Representative will need to complete and submit a new application in accordance with Section 3.1.8.1 (a) or (b).

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

4. OPERATIONAL REQUIREMENTS

4.1 d-Cert (Personal) Certificates

4.1.1 Certificate Application

4.1.1.1 Application Processing

4.1.1.1.1 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**).

4.1.1.1.2 For a d-Cert (Personal) certificate, the Applicant must, at the time of application, accept to use the PKCS#12 format file for issuance of the d-Cert and Private Key. If the d-Cert application is submitted through the d-Cert Subscriber Portal, the Applicant must also agree to download the file via the portal. Otherwise, the file will be stored on a d-Cert File USB, serving as the d-Cert Storage Medium.

4.1.1.1.3 For a d-Cert (Personal) certificate that supports Adobe PDF signing, the Applicant must, at the time of application, choose a PKCS#11 compliant device as the d-Cert Storage Medium for issuance of the d-Cert and the Private Key.

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

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

4.1.1.2 Identity Verification

The Applicant is required to present valid proof of identity through one of the processes described in Section 3.1.9(a), (b) and (c). Upon satisfactory completion of the identity verification process, HKCA will generate the PIN for accessing the d-Cert (Personal) certificate (including the associated key pairs) to be issued. The d-Cert PIN will be required for any subsequent use of the d-Cert and Private Key to prevent unauthorised access.

4.1.2 Certificate Issuance

4.1.2.1 Issuance of d-Cert (Personal) certificate through d-Cert Subscriber Portal

4.1.2.1.1 Following the identity verification process, HKCA will generate the d-Cert (including the associated key pairs) of the respective Applicants in a Trustworthy System and environment within HKCA's designated premises to ensure that the Private Key will not be tampered with.

4.1.2.1.2 The Private Key and d-Cert will then be stored in a PKCS#12 format file ("d-Cert File") for download by the Applicant or on a d-Cert File USB, which will serve as the d-Cert Storage Medium. If a PKCS#11-compliant device is selected as the d-Cert Storage Medium, the Private Key and d-Cert will be issued directly on the PKCS#11-compliant device (refer to Section 4.1.2.2).

4.1.2.1.3 Each d-Cert File will be protected by an associated PIN. A secure electronic link for retrieval of the PIN will be sent separately to the Applicant by email. Any subsequent use of the d-Cert and Private Key contained in the d-Cert File will require the associated PIN to ensure unauthorized access is prevented.

4.1.2.1.4 The d-Cert File will be temporarily maintained in the d-Cert Subscriber Portal, allowing the Applicant to download it.

4.1.2.1.5 The accepted and issued d-Cert will then be published in the Repository.

4.1.2.1.6 The Applicant must log in to the d-Cert Subscriber Portal and then download the d-Cert File to their local system storage. Once the Applicant has downloaded the d-Cert File and retrieved the associated PIN, the d-Cert Subscriber Portal will permanently delete both.

4.1.2.2 Issuance of d-Cert (Personal) certificate in d-Cert Storage Medium

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

4.1.2.2.2 The Private Key and d-Cert will then be stored in the d-Cert Storage Medium selected by the Applicant.

4.1.2.2.3 Each d-Cert Storage Medium will be protected by an associated PIN. A secure electronic link for retrieval of the PIN will be sent separately to the Applicant by email. Any subsequent use of the d-Cert and Private Key contained in the d-Cert Storage Medium will require the associated PIN to ensure unauthorized access is prevented.

4.1.2.2.4 The d-Cert Storage Medium will be securely sealed in a tamper-proof envelope or other forms of containers and delivered to the Applicant in a secure manner such as by registered mail.

4.1.2.2.5 The accepted and issued d-Cert will then be published in the Repository.

4.1.2.3 Private Keys

4.1.2.3.1 The d-Cert and the Private Key cannot be recovered from HKCA if lost or damaged. As such, the Applicant is responsible for maintaining the d-Cert File or the d-Cert Storage Medium as a backup of their d-Cert and Private Key.

4.1.2.3.2 All Private Keys stored in the d-Cert Subscriber Portal and HKCA system are in encrypted form. Proper security controls are in place to guard against unauthorised access to and disclosure of the encrypted Private Keys. Upon completion of delivery of the d-Certs and Private Keys to the Applicants, the relevant Private Keys will be purged from the d-Cert Subscriber Portal and HKCA system.

4.1.2.4 Verification on Certificate Information

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

4.1.3 Publication of d-Cert

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

4.2 d-Cert (Organisational) Certificates

4.2.1 Certificate Application

4.2.1.1 Application Processing

4.2.1.1.1 Applicants for d-Cert (Organisational) certificates must submit their d-Cert applications, including any supplementary application forms and all supporting documents as required by the HKCA, either through the d-Cert Subscriber Portal, or through the Contractor or a RA, where applicable (see **Appendix E**).

4.2.1.1.2 For a d-Cert (Organisational) certificate, the Applicant must, at the time of application, accept to use the PKCS#12 format file for issuance of the d-Cert and Private Key. If the d-Cert application is submitted through the d-Cert Subscriber Portal, the Applicant must also agree to download the files via the portal. Otherwise, the file will be stored on a d-Cert File USB, serving as the d-Cert Storage Medium.

4.2.1.1.3 For a d-Cert (Organisational) certificate that supports Adobe PDF signing, the Applicant must, at the time of application, choose a PKCS#11 compliant device as the d-Cert Storage Medium for issuance of the d-Cert and the Private Key.

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

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

4.2.1.2 Identity Verification

The documentation required for proving the identity of the Subscriber Organisation, Authorised Representative(s) and Authorised Users is stipulated in Section 3.1.8 of this CPS. Upon satisfactory completion of the identity verification process, HKCA will generate the PINs for accessing the d-Cert (Organisational) certificates (including the associated key pairs) to be issued to the respective Authorised Users. The d-Cert PIN will be required for any subsequent use of the d-Cert and Private Key to prevent unauthorised access.

4.2.2 Certificate Issuance

4.2.2.1 Issuance of d-Cert (Organisational) certificate through d-Cert Subscriber Portal

4.2.2.1.1 Following the identity verification process, HKCA will generate the d-Certs (including the associated key pairs) of the respective Authorised Users in a Trustworthy System

and environment within HKCA's designated premises to ensure that the Private Key will not be tampered with.

4.2.2.1.2 The Private Key and d-Cert for each Authorised User will then be stored in an individual PKCS#12 format file ("d-Cert File") for download by the Authorised Representative(s) or on a d-Cert File USB, which will serve as the d-Cert Storage Medium. If a PKCS#11-compliant device is selected as the d-Cert Storage Medium, the Private Key and d-Cert will be issued directly on the PKCS#11-compliant device (refer to Section 4.2.2.2).

4.2.2.1.3 The Authorised Representative is responsible for distributing each d-Cert File to the respective Authorised User. The d-Cert File will be protected by the associated PIN, and a secure electronic link for retrieval of the PIN will be sent separately to the respective Authorised Users by email. Any subsequent use of the d-Cert and Private Key contained in the d-Cert File will require the associated PIN to ensure unauthorized access is prevented.

4.2.2.1.4 The d-Cert File will be temporarily maintained in the d-Cert Subscriber Portal, allowing the Authorised Representative to download it.

4.2.2.1.5 The accepted and issued d-Cert will then be published in the Repository.

4.2.2.1.6 The Authorised Representative must log in to the d-Cert Subscriber Portal and then download the d-Cert File to their local system storage. Once the Authorised Representative has downloaded the d-Cert File and the respective Authorised User has retrieved the associated PIN, the d-Cert Subscriber Portal will permanently delete both.

4.2.2.2 Issuance of d-Cert (Organisational) certificate in d-Cert Storage Medium

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

4.2.2.2.2 The Private Key and d-Cert will then be stored on the d-Cert Storage Medium selected by the Authorised Representative.

4.2.2.2.3 Each d-Cert Storage Medium will be protected by an associated PIN. A secure electronic link for retrieval of the PIN will be sent separately to the respective Authorised User by email. Any subsequent use of the d-Cert and Private Key contained in the d-Cert Storage Medium will require the associated PIN to ensure unauthorized access is prevented.

4.2.2.2.4 The d-Cert Storage Medium will be securely sealed in a tamper-proof envelope or other forms of containers and delivered to the Applicant in a secure manner such as by registered mail.

4.2.2.2.5 The accepted and issued d-Cert will then be published in the Repository.

4.2.2.3 Private Keys

4.2.2.3.1 The d-Cert and the Private Key cannot be recovered from HKCA if lost or damaged. As such, the Applicant is responsible for maintaining the d-Cert File or the d-Cert Storage Medium as a backup of their d-Cert and Private Key.

4.2.2.3.2 All Private Keys stored in the d-Cert Subscriber Portal and HKCA system are in encrypted form. Proper security controls are in place to guard against unauthorised access to and disclosure of the encrypted Private Keys. Upon completion of delivery of the d-Certs and Private Keys to the Applicants, the relevant Private Keys will be purged from the d-Cert Subscriber Portal and HKCA system.

4.2.2.4 Verification on Certificate Information

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

4.2.3 Publication of d-Cert

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

4.3 d-Cert (Encipherment) Certificates

4.3.1 Certificate Application

4.3.1.1 Application Processing

4.3.1.1.1 Applicants for d-Cert (Encipherment) certificates must submit their d-Cert applications, including any supplementary application forms and all supporting documents as required by the HKCA, either through the d-Cert Subscriber Portal, or through the Contractor or a RA, where applicable (see **Appendix E**).

4.3.1.1.2 The Applicant must, at the time of application, accept to use the PKCS#12 format file for issuance of the d-Cert and Private Key. If the d-Cert application is submitted through the d-Cert Subscriber Portal, the Applicant must also agree to download the files via the portal. Otherwise, the file will be stored on a d-Cert File USB, serving as the d-Cert Storage Medium.

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

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

4.3.1.2 Identity Verification

The documentation required for proving the identity of the Subscriber Organisation, Authorised Representative(s) and Authorised Users is stipulated in Section 3.1.8 of this CPS. Upon satisfactory completion of the identity verification process, HKCA will generate the PINs for accessing the d-Cert (Encipherment) certificates (including the associated key pairs) to be

issued to the respective Authorised Units. The d-Cert PIN will be required for any subsequent use of the d-Cert and Private Key to prevent unauthorised access.

4.3.2 Certificate Issuance

4.3.2.1 Issuance of d-Cert (Encipherment) certificate through d-Cert Subscriber Portal

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

4.3.2.1.2 The Private Key and d-Cert for each Authorised Unit will then be stored in an individual PKCS#12 format file ("d-Cert File") for download by the Authorised Representative(s) or on a d-Cert File USB, which will serve as the d-Cert Storage Medium (refer to Section 4.3.2.2).

4.3.2.1.3 The Authorised Representative is responsible for distributing each d-Cert File to the respective Authorised Unit. The d-Cert File will be protected by the associated PIN, and a secure electronic link for retrieval of the PIN will be sent separately to the respective Authorised Units by email. Any subsequent use of the d-Cert and Private Key contained in the d-Cert File will require the associated PIN to ensure unauthorized access is prevented.

4.3.2.1.4 The d-Cert File will be temporarily maintained in the d-Cert Subscriber Portal, allowing the Authorised Representative to download it.

4.3.2.1.5 The accepted and issued d-Cert will then be published in the Repository.

4.3.2.1.6 The Authorised Representative must log in to the d-Cert Subscriber Portal and then download the d-Cert File to their local system storage. Once the Authorised Representative has downloaded the d-Cert File and the respective Authorised Unit has retrieved the associated PIN, the d-Cert Subscriber Portal will permanently delete both.

4.3.2.2 Issuance of d-Cert (Encipherment) certificate in d-Cert Storage Medium

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

4.3.2.2.2 The Private Key and d-Cert will then be stored on the d-Cert Storage Medium selected by the Authorised Representative.

4.3.2.2.3 Each d-Cert Storage Medium will be protected by an associated PIN. A secure electronic link for retrieval of the PIN will be sent separately to the respective Authorised Unit by email. Any subsequent use of the d-Cert and Private Key contained in the d-Cert Storage Medium will require the associated PIN to ensure unauthorized access is prevented.

4.3.2.2.4 The d-Cert Storage Medium will be securely sealed in a tamper-proof envelope or other forms of containers and delivered to the Applicant in a secure manner such as by registered mail.

4.3.2.2.5 The accepted and issued d-Cert will then be published in the Repository.

4.3.2.3 Private Keys

4.3.2.3.1 The d-Cert and the Private Key cannot be recovered from HKCA if lost or damaged. As such, the Applicant is responsible for maintaining the d-Cert File or the d-Cert Storage Medium as a backup of their d-Cert and Private Key.

4.3.2.3.2 All Private Keys stored in the d-Cert Subscriber Portal and HKCA system are in encrypted form. Proper security controls are in place to guard against unauthorised access to and disclosure of the encrypted Private Keys. Upon completion of delivery of the d-Certs and Private Keys to the Applicants, the relevant Private Keys will be purged from the d-Cert Subscriber Portal and HKCA system.

4.3.2.4 Verification on Certificate Information

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

4.3.3 Publication of d-Cert

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

4.4 Timeframe for Processing Certificate Applications

HKCA will 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**
d-Cert (Personal)	Three working days
d-Cert (Organisational)	Ten working days
d-Cert (Encipherment)	

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 4.4.

4.5 Certificate Suspension and Revocation

4.5.1 Circumstances for Suspension and Revocation

4.5.1.1 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 4.10.2).

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

4.5.1.3 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 (see also Section 2.1.4(k)).

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

a) knows or reasonably suspects that a Subscriber's Private Key has been compromised;
b) knows or reasonably suspects that any details upon a certificate are not true or have become untrue or that the certificate is otherwise unreliable;
c) determines that a certificate was not properly issued in accordance with the CPS;
d) determines that the Subscriber had failed to meet any of the obligations set out in this CPS or the Subscriber Agreement;
e) is required to do so by any regulation, or law applicable to the certificate;
f) determines that the Subscriber has failed to pay the subscription fee;
g) knows or has reasonable cause to believe that the Subscriber whose details appear on a d-Cert (Personal) certificate:
   (i) is dead or has died;
   (ii) is or has become an undischarged bankrupt or has entered into a composition or scheme of arrangement or a voluntary arrangement within the meaning of the Bankruptcy Ordinance (Cap. 6) within 5 years preceding the date of revocation; or
   (iii) has been convicted in Hong Kong or elsewhere of an offence for which it was necessary to find that the person acted fraudulently, corruptly or dishonestly or committed an offence under the Electronic Transactions Ordinance;
h) knows or has reasonable cause to believe that the Authorised User named in a d-Cert (Organisational) certificate has ceased to be a member or employee of the Subscriber Organisation;
i) knows or has reasonable cause to believe that the Subscriber whose details appear on a d-Cert (Organisational), or d-Cert (Encipherment) certificate that:

   (i) the Subscriber is in liquidation, or a winding up order relating to the Subscriber has been made by any Court of competent jurisdiction;
   (ii) the Subscriber has entered into a composition or a scheme of arrangement or a voluntary arrangement within the meaning of the Bankruptcy Ordinance (Cap.6) within 5 years preceding the date of intended revocation;
   (iii) a director, officer or employee of the Subscriber has been convicted of an offence for which it was necessary to find that that person acted fraudulently, corruptly or dishonestly or committed an offence under the Electronic Transactions Ordinance;

(iv) a receiver or administrator has been appointed over any part of the Subscriber's assets within 5 years preceding the date of revocation; or
(v) the Subscriber's existence cannot be attested.

4.5.1.5 HKCA will 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.

4.5.2 Revocation Request Procedure

A Subscriber, or the Authorised Representative of a Subscriber Organisation, may submit a certificate revocation request to HKCA through a designated web page on the HKCA website, d-Cert Subscriber Portal, email or in-person.

After receiving the revocation request, HKCA will validate the request and verify the justifications for revocation before suspending the certificate. The certificate will be revoked, which terminates the validity of the certificate permanently, upon receipt of the final confirmation of revocation from the Subscriber or from the RA to which the request for revocation was first submitted. Final confirmation may be one of the following: an acknowledgement on the d-Cert Subscriber Portal, an email digitally signed by the Subscriber's Private Key, or an original letter signed by the Subscriber or a Request for Certificate Revocation Form signed by the Subscriber. The Request for Certificate Revocation Form is available from the HKCA website.

If no final confirmation of revocation is received from the Subscriber, the certificate will remain suspended and will be included in the Certificate Revocation List (CRL) until it expires. HKCA may consider requests from Subscribers to resume suspended certificates. However, any decision to resume validity is at HKCA's sole discretion.

Information for all certificates that have been suspended or revoked, including a reason code identifying the cause of suspension or revocation, will be included in the Certificate Revocation List (see Section 7.2). A certificate resumed from "suspended" status will not appear in subsequent Certificate Revocation Lists.

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.

4.5.3 Service Pledge & Update of Certificate Revocation List

a) HKCA will exercise reasonable endeavours to ensure that the suspension or revocation

of a certificate is posted to the Certificate Revocation List (CRL) within two (2) working days of either (1) receiving a revocation request or final confirmation of revocation from the Subscriber, or (2) HKCA's decision to suspend or revoke the certificate in the absence of such a request.

A CRL is not published to the public directory immediately after each suspension or revocation. The suspended or revoked status will be reflected only when the next CRL is updated and published. CRLs are published daily and are archived for at least seven (7) years.

For the avoidance of doubt, all Saturdays, Sundays, public holidays and for all weekdays on which a tropical cyclone warning signal no. 8 (or above) or a black rainstorm warning signal is hoisted, are not working days for the purpose of this section 4.5.3 (a).

HKCA will exercise reasonable endeavors to notify relevant Subscribers by updating the CRL, and by email, if a contact email address is available, within two (2) working days following the suspension or revocation.

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

c) Further, upon becoming so aware of any ground upon which 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 will 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 will be under no liability to Relying Parties in respect of the transactions in the period between HKCA's decision to suspend or revoke a certificate (either in response to a request or otherwise) and the appearance of the suspension or revocation status on the CRL, or in the period between that decision to suspend or revoke a certificate, 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.

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

e) The Certificate Revocation List ("CRL"), Authority Revocation List ("ARL") of HKCA are updated and published in accordance with the schedule and format specified in

Appendix C.

f) HKCA's policy concerning the situation where a Relying Party is temporarily unable to obtain Information on suspended or revoked certificate is stipulated in Section 2.1.6 (Relying Parties Obligations) and Section 2.2.1 (Reasonable Skill and Care) of this CPS.

4.5.4 Effect of Revocation

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

4.6 Termination of Certificate 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 subscription 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 Archive Retention Period specified in Section 4.8.2.

4.7 Computer Security Audit Procedures

4.7.1 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:

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

4.7.2 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.

4.7.3 Retention Period for Audit Logs

Archived audit log files are retained for 7 years.

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

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

4.7.6 Audit Information Collection System
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.

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

4.7.8 Vulnerability Assessments
Vulnerability assessments are conducted as part of HKCA's CA security procedures.

4.8 Records Archival

4.8.1 Types of Records Archived
HKCA will 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:

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

4.8.2 Archive Retention Period
Key and certificate information as well as archival records as specified in Section 4.8.1 are securely maintained for at least 7 years. Audit trail files are maintained in the CA system as deemed appropriate by HKCA.

4.8.3 Archive Protection
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.

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

4.8.5 Timestamping
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.

4.9 Key Changeover

The lifespan of the HKCA and d-Cert root keys and certificates created by HKCA (See **Appendix G**) 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 website for public access. The original root keys will be kept for a minimum period as specified in Section 4.8.2 for verification of any signatures generated by the original root keys. HKCA will ensure safe and smooth transition of the entire process, with a view to minimizing the adverse effects on Subscribers and Relying Parties.

4.10 Disaster Recovery and Key Compromise Plans

4.10.1 Disaster Recovery Plan
A managed process, including daily backup of essential business information and CA system data and proper backup of CA system software, is in place for maintaining business continuity plans to protect critical business processes from the effect of major failures or disasters. Business continuity plans exist to enable the complete recovery of all 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 will promptly notify the Commissioner for Digital Policy and make public announcement of the switchover of operation from the production site to the disaster recovery site as a result of major failures or disasters.

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

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

4.10.2 Key Compromise Plan

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

HKCA will promptly notify the Commissioner for Digital Policy and make public announcement if a HKCA Private Key for the issuance of d-Cert 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 will timely and properly inform Subscribers and Relying Parties within a reasonable period of time.

4.10.3 Key Replacement

In the event of key compromise or disaster where a HKCA Private Key for the issuance of d-Cert certificates under this CPS has been compromised or corrupted and cannot be recovered, HKCA will 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 will only proceed subject to the confirmation of the Commissioner for Digital Policy.

4.10.4 Damaged Computing Resources, Software and/or Data

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

When computing resources, software and/or data are damaged, HKCA will 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 certificates under this CPS has been compromised or damaged, HKCA will 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 will promptly revoke the respective certificates and issue new and replacement certificates. HKCA will timely and properly inform Subscribers and Relying Parties within a reasonable period of time.

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

4.12 RA Termination

In the event that the RA is terminated under RA agreement or under CA termination (see Section 4.11) 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.

5. PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY CONTROLS

5.1 Physical Security

5.1.1 Site Location and Construction

The HKCA is located within data centres that affords commercially reasonable physical security. The data centres are equipped with logical and physical controls that make HKCA operations inaccessible to non-trusted personnel. HKCA operates under a security policy designed to detect, deter, and prevent unauthorized access to HKCA operations.

5.1.2 Access Controls

5.1.2.1 Data Centres

HKCA protects its equipment from unauthorized access and implements physical controls to reduce the risk of equipment tampering. The data centres where HKCA systems operate have security personnel on duty full time (24 hours per day, 365 days per year). Access to the data centres housing the CA platforms requires two-factor authentication— the individual must have an authorized access card and pass biometric access control authenticators. These biometric authentication access systems log each use of the access card.

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 will 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 will be retained for at least 3 months.

5.1.2.1 RA Operation Areas

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 will ensure that access to each physical security layer is auditable and controllable so that only authorised personnel can access each physical security layer.

5.1.3 Environmental controls of Computer Cabinet

The HKCA data centres are continuously attended. However, if HKCA ever becomes aware that a data centre is to be left unattended or has been left unattended for an extended period of time, HKCA personnel will perform a security check of the data centre to verify that:

a) HKCA's equipment is in a state appropriate to the current mode of operation,
b) Any security containers are properly secured,
c) Physical security systems (e.g., computer cabinet locks) are functioning properly, and
d) The area is secured against unauthorized access.

Monitoring system is in place to provide physical security monitoring of the data centre for infrastructure equipment, computer cabinets and security protection system 24 hours a day and seven days a week. The monitoring records will be retained for 3 months for the purposes of fault diagnosis and post-event auditing.

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

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

5.1.6 Fire and Flooding Prevention and Protection
The data centres are equipped with fire suppression mechanisms including, installed fire fighting equipment and smoke and temperature detectors. All fire-protection measures comply with the requirements specified by Fire Services Department of Hong Kong. The fire alarm system and the fire extinguishing system have been linked together. The cabinets housing HKCA systems are located on raised flooring, and the data centres have monitoring systems in place to detect flooding and water leakage.

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

5.1.8 Off-site Backup
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 4.10.1).

5.1.9 Custody of Subscriber Agreements and Other Documents
Subscriber Agreements and identity confirmation documents submitted electronically are securely maintained by HKCA, its Contractor, or its RAs in accordance with applicable data protection and security policies. Only authorised personnel are permitted access to these records and appropriate safeguards are in place to prevent unauthorised access or disclosure.

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

5.2 Procedural Controls

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

Procedures are established, documented and implemented for all trusted roles in relation to 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.

5.2.2 Transfer of Document and Data between HKCA, Contractor and RAs

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.

5.2.3 Annual Assessment

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

5.3 Personnel Controls

5.3.1 Background and Qualifications

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 Investigation

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 will 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 will provide appropriate and sufficient training for their staff (at least once a year for those holding core positions) to ensure their capabilities in carrying their duties as well as effective implementation and compliance with security policies. The content of training may include but not limited to:

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

5.3.4 Assessment of Existing Staff

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

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

5.3.5 Documentation Supplied To Personnel

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.

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 key pairs for issuing certificates that conform to this CPS. In case of central key generation by HKCA on behalf of the Applicants, the Applicants' Private Keys will be purged from the HKCA system upon completion of delivery of the d-Certs and Private Keys to the Applicants.

6.1.2 Subscriber Private Key Delivery

Key pairs for d-Cert (Personal), d-Cert (Organisational) and d-Cert (Encipherment) certificates will be generated under the central key generation by HKCA on behalf of the Applicant/Subscriber.

6.1.3 Public Key Delivery to Subscriber

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.

6.1.4 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

6.1.5 Standards for Cryptographic Module

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

6.1.6 Key Usage Purposes

Keys used in d-Cert (Personal), d-Cert (Organisational) and d-Cert (Encipherment) certificates may be used for Digital Signatures and conducting enciphered electronic communications. HKCA Root Key (the key used to create or issue certificates that conform to this CPS) is used only for Digital Signatures such as signing (a) certificates and (b) Certificate Revocation Lists.

6.2 Private Key Protection

6.2.1 Standards for Cryptographic Module
HKCA Private Keys are created in a crypto module validated to at least FIPS 140-2 Level 3.

6.2.2 Private Key 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 Backup of HKCA Private Keys
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. All Private Keys will not be archived.

6.2.5 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 authorization.

6.3 Other Aspects of Key Pair Management

HKCA root keys will be used for no more than the lifespan of the respective signing root key and certificates created by HKCA (see **Appendix G** and also Section 4.9). All HKCA key generation, key destruction, key storage, certificate revocation list signing operations are performed in a hardware cryptographic module. Archival of HKCA Public Keys is performed as specified in Section 4.8.

6.4 Computer Security Controls

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 2.6. 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 Life Cycle Technical Security 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 will 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 Network Security Controls

HKCA will 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 will be conducted in order to detect intrusion risks and minimize risks from the network.

6.7 Cryptographic Module Engineering Controls

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

7. CERTIFICATE PROFILE, CERTIFICATE REVOCATION LIST

7.1 Certificate Profile

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

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

7.2 Certificate Revocation List Profile

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

8. CPS ADMINISTRATION

All changes to this CPS must be approved and published by HKCA. The CPS changes will be effective upon publication by HKCA in the HKCA website or in the Repository and are binding on all current and subsequent Applicants and Subscribers to whom certificates are issued. HKCA will notify the Commissioner for Digital Policy any subsequent changes to this CPS as soon as practicable. A copy of this CPS and its predecessors are available for viewing by Applicants, Subscribers and Relying Parties on the HKCA website.

Appendix A - Glossary

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

"Accept", in relation to a certificate

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

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

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

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

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

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

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

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

"CA" means Certification Authority.

"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 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.

"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 F**, 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.

"d-Cert File USB" means a USB flash drive which is a d-Cert Storage Medium. The prevailing cost of a d-Cert File USB is published at HKCA website.

"d-Cert Storage Medium" means a storage medium, such as d-Cert File USB or PKCS#11 compliant device, for storage of the d-Cert and the Private Key.

"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.

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

"iAM Smart+" means the enhanced version of the "iAM Smart" digital identity platform provided by the Hong Kong SAR Government. It includes digital signing functionality that comply with the Electronic Transactions Ordinance (Cap. 553), enabling users to create legally recognized electronic signatures.

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

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

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

"IRD Reference Number" means a number being assigned by the Inland Revenue Department to a Reporting Financial Institution / Reporting Entity as referred in the Inland Revenue Ordinance (Cap. 112). The IRD Reference Number will be given in a certification letter issued to the Reporting Financial Institution / Reporting Entity issued by Inland Revenue Department.

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

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

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

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

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

"PKCS#11 compliant device" means a device, such as smart card, which is a storage medium of d-Cert and supports cryptographic functions, and also complies to the eleventh specification of the Public-Key Cryptography Standards (PKCS) published by RSA Laboratories, in respect of cryptographic token interface standard. Such device should also be certified with FIPS 140-2 Level 3 or above.

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

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

"RA" means Registration Authority.

"Recognized CA" means Recognized Certification Authority.

"Recognized Certificate" means

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

"Recognized Certification Authority" means a Certification Authority recognized under the Voluntary CA Recognition Scheme pursuant to the Electronic Transactions Ordinance.

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

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

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

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

"Repository" means an Information System of HKCA 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.

"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 between the Subscriber and HKCA comprising the subscriber terms and conditions submitted with the application and the provisions of 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 certificate has been issued in accordance with the eligibility criteria set out in this CPS.

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

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

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

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

Appendix B - HKCA d-Cert Format

This appendix provides the formats of d-Cert issued by the Sub CAs "HKCA d-Cert CA 1 - 25" and "HKCA d-Cert CA 1 - 25A" 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 (Personal) Certificate

1.1 Under root CA "HKCA Root CA 1"

For d-Cert (Personal) issued by Sub CA "HKCA d-Cert CA 1 - 25": -

Field Name		**Field Content**	
		HKCA d-Cert (Personal) certificates	**HKCA d-Cert (Personal) certificates issued to persons aged under 18**
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 CA 1 - 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=[HKID name] (Note 1) e=[email address] (Note 2) ou=[SRN] (Note 3) o=HKCA d-Cert (Personal) c=HK	cn=[HKID name] (Note 1) e=[email address] (Note 2) ou=[SRN] (Note 3) o=HKCA d-Cert (Personal/Minor) (Note 4) c=HK
Subject public key info		Algorithm ID: RSA Public Key: 2048-bit key size	
Issuer unique identifier		Not used	
Subject unique identifier		Not used	
Standard extension (Note 5)			
Authority Key Identifier		[Subject Key Identifier of the issuer's certificate]	
Key usage		Non-repudiation, Digital Signature, Key Encipherment **(This field will be set Critical.)**	
Certificate policies		Policy Identifier = [OID] (Note 6) Policy Qualifier Id = CPS Qualifier : [URL of CPS]	
Subject alternative name	**DNS**	encrypted(HKID) (Note 10)	
	rfc822	[Applicant's email address] (Note 2)	
Issuer alternative name		Not used	
Basic constraints	**Subject type**	End Entity	
	Path length constraint	None	
Extended key usage		SSL Client, S/MIME	
CRL distribution points		Distribution Point Name = [URL of CRL Distribution Point] (Note 11)	

Field Name		Field Content	
		HKCA d-Cert (Personal) certificates	HKCA d-Cert (Personal) certificates issued to persons aged under 18
Netscape extension (Note 5)			
Netscape cert type		Not used	
Netscape SSL server name		Not used	
Netscape comment		Not used	

For d-Cert (Personal) that supports Adobe PDF signing, issued by Sub CA "HKCA d-Cert CA 1 - 25A": -

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 CA 1 – 25A, 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=[HKID name] (Note 1) e=[email address] (Note 2) ou=[SRN] (Note 3) o=HKCA d-Cert (Personal) c=HK
Subject public key info		Algorithm ID: RSA Public Key: 2048-bit key size
Issuer unique identifier		Not used
Subject unique identifier		Not used
Standard extension (Note 5)		
Authority Key Identifier		[Subject Key Identifier of the issuer's certificate]
Key usage		Non-repudiation, Digital Signature **(This field will be set Critical.)**
Certificate policies		Policy Identifier =[OID] (Note 6) Policy Qualifier Id = CPS Qualifier : [URL of CPS] Policy Identifier = 1.3.6.1.4.1.64092.1.4 (Note 9) Policy Qualifier Id = CPS Qualifier : [URL of CPS]
Subject alternative name	**DNS**	encrypted(HKID) (Note 10)
	Rfc822	[Applicant's email address] (Note 2)
Issuer alternative name		Not used
Basic constraints	**Subject type**	End Entity
	Path length constraint	None
Extended key usage		SSL Client, S/MIME
CRL distribution points		Distribution Point Name = [URL of CRL Distribution Point] (Note 12)
Netscape extension (Note 5)		
Netscape cert type		Not used
Netscape SSL server name		Not used
Netscape comment		Not used

Note

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

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

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

    With Central Key Generation, hkid_number will be signed during the key generation process at HKCA's designated premises and the CA system will create a hash of the signed HKID number - ***SHA-1*** ($RSA_{privatekey,\ sha\text{-}1}$ (hkid_number)). The hash value will then be put into the designated extension field of the certificate being generated.
11. URL of CRL Distribution Point is http://crl.hkca.hk/crl/HKCAdCertCA1-25CRL_<xxxxx>.crl which are partitioned CRLs issued by the Sub CA "HKCA d-Cert CA 1 - 25", where <xxxxx> is a string of five alphanumeric characters generated by the CA system. HKCA publishes several partitioned CRLs for this type of certificate. If a certificate is suspended or revoked, its information will be published in the partitioned CRL at the URL specified in this CRL Distribution Point field.
12. URL of CRL Distribution Point is http://crl.hkca.hk/crl/HKCAdCertCA1-25ACRL_<xxxxx>.crl which are partitioned CRLs issued by the Sub CA "HKCA d-Cert CA 1 - 25A", where <xxxxx> is a string of five alphanumeric characters generated by the CA system. HKCA publishes several partitioned CRLs for this type of certificate. If a certificate is suspended or revoked, its information will be published in the partitioned CRL at the URL specified in this CRL Distribution Point field.

2. Format of d-Cert (Organisational) Certificate

2.1 Under root CA "HKCA Root CA 1"

For d-Cert (Organisational) issued by Sub CA "HKCA d-Cert CA 1 - 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 CA 1 - 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=[Authorised User's name] (Note 1) e=[email address] (Note 2) ou=[SRN] (Note 3) ou=[(BRN or IRD Reference Number)+CI/CR+Others] (Note 4) ou=[Subscriber Organisation Name] (Note 5) ou=[Subscriber Organisation branch/dept] (Note 5) o=HKCA d-Cert (Organisational) c=HK
Subject public key info		Algorithm ID: RSA Public Key: 2048-bit key size
Issuer unique identifier		Not used
Subject unique identifier		Not used
Standard extension (Note 6)		
Authority Key Identifier		[Subject Key Identifier of the issuer's certificate]
Key usage		Non-repudiation, Digital Signature, Key Encipherment **(This field will be set Critical.)**
Certificate policies		Policy Identifier = [OID] (Note 7) Policy Qualifier Id = CPS Qualifier : [URL of CPS]
Subject alternative name	**DNS**	[0 to 10 application-specific code(s)] (Note 10)
	First Directory Name	ou=[Subscriber Organisation's Chinese name] (Note 5) ou=[Subscriber Organisation's Chinese branch/dept name] (Note 5)
	Rfc822	[Applicant's email address] (Note 2)
Issuer alternative name		Not used
Basic constraints	**Subject type**	End Entity
	Path length constraint	None
Extended key usage		SSL Client, S/MIME
CRL distribution points		Distribution Point Name = [URL of CRL Distribution Point] (Note 11)
Netscape extension (Note 6)		
Netscape cert type		Not used
Netscape SSL server name		Not used
Netscape comment		Not used

For d-Cert (Organisational) that supports Adobe PDF signing, issued by Sub CA "HKCA d-Cert CA 1 - 25A": -

Field Name		Field Content
Standard fields		
Version		X.509 v3

Field Name		Field Content
Serial number		[20-byte hexadecimal number set by HKCA system]
Signature algorithm ID		sha256RSA
Issuer name		cn=HKCA d-Cert CA 1 - 25A, 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=[Authorised User's name] (Note 1) e=[email address] (Note 2) ou=[SRN] (Note 3) ou=[(BRN or IRD Reference Number)+CI/CR+Others] (Note 4) ou=[Subscriber Organisation Name] (Note 5) ou=[Subscriber Organisation branch/dept] (Note 5) o=HKCA d-Cert (Organisational) c=HK
Subject public key info		Algorithm ID: RSA Public Key: 2048-bit key size
Issuer unique identifier		Not used
Subject unique identifier		Not used
Standard extension (Note 6)		
Authority Key Identifier		[Subject Key Identifier of the issuer's certificate]
Key usage		Non-repudiation, Digital Signature **(This field will be set Critical.)**
Certificate policies		Policy Identifier =[OID] (Note 7) Policy Qualifier Id = CPS Qualifier : [URL of CPS] Policy Identifier = 1.3.6.1.4.1.64092.1.4(Note 9) Policy Qualifier Id = CPS Qualifier : [URL of CPS]
Subject alternative name	**DNS**	[0 to 10 application-specific code(s)] (Note 10)
	First Directory Name	ou=[Subscriber Organisation's Chinese name] (Note 5) ou=[Subscriber Organisation's Chinese branch/dept name] (Note 5)
	Rfc822	[Applicant's email address] (Note 2)
Issuer alternative name		Not used
Basic constraints	**Subject type**	End Entity
	Path length constraint	None
Extended key usage		SSL Client, S/MIME
CRL distribution points		Distribution Point Name = [URL of CRL Distribution Point] (Note 12)
Netscape extension (Note 6)		
Netscape cert type		Not used
Netscape SSL server name		Not used
Netscape comment		Not used

Note

1. Authorised User name format: Surname (in capital) + Given name (e.g. CHAN Tai Man David).
2. Email address provided by Authorised User (blank if null). That email address has not been verified.
3. SRN: 10-digit Subscriber Reference Number
4. Business Registration Certificate Number (BRN): a string of 16 digits/alphabets [filled with all zeroes if BRN is not available]. Alternatively for organisations who present a copy of certification letter issued by the Inland Revenue Department in place of a copy of Business Registration Certificate, the IRD Reference Number of the certification letter, which is a string of 8 digits/alphabets, together with 8 trailing zeros, is included in

BRN field. Certificate of Incorporation (CI)/ Certificate of Registration (CR): a string of 8 digits/alphabets [filled with leading zeros if CI/CR is shorter than 8 digits/alphabets, all zeroes if CI/CR is not available, or all zeros for Limited Partnership Fund (LPF)]. Others: a string of max. 30 digits/alphabets (blank if null). For HKSAR government departments, BRN and CI/CR are filled with zeroes, department name in abbreviation (e.g. DPO for Digital Policy Office) is placed in Others. For an organisation who is registered as an LPF under the Limited Partnership Fund Ordinance (Cap. 637), the respective CR is placed in Others.

5. For organisations who subscribe to d-Cert and are companies with company names in the Chinese language only, a default name "***CHINESE NAME ONLY***" will be set for the company's English name. In all circumstances when the company's Chinese name is provided and verified by HKCA, it will be included in the First Directory Name of the Subject Alternative Name field (see Section 3.1.1.6 of this CPS). Chinese name must adopt the international coding standard ISO/IEC 10646.

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

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

8. Reserved for future use.

9. The OID for supporting Adobe PDF signing is added in this field.

10. The application-specific code for particular application is defined in this field (see **Appendix H**).

11. URL of CRL Distribution Point is http://crl.hkca.hk/crl/HKCAdCertCA1-25CRL_<xxxxx>.crl which are partitioned CRLs issued by the Sub CA "HKCA d-Cert CA 1 - 25", where <xxxxx> is a string of five alphanumeric characters generated by the CA system. HKCA publishes several partitioned CRLs for this type of certificate. If a certificate is suspended or revoked, its information will be published in the partitioned CRL at the URL specified in this CRL Distribution Point field.

12. URL of CRL Distribution Point is http://crl.hkca.hk/crl/HKCAdCertCA1-25ACRL_<xxxxx>.crl which are partitioned CRLs issued by the Sub CA "HKCA d-Cert CA 1 - 25A", where <xxxxx> is a string of five alphanumeric characters generated by the CA system. HKCA publishes several partitioned CRLs for this type of certificate. If a certificate is suspended or revoked, its information will be published in the partitioned CRL at the URL specified in this CRL Distribution Point field.

3. d-Cert (Encipherment) Certificate Format

3.1 Under root CA "HKCA Root CA 1"

For d-Cert (Encipherment) issued by Sub CA "HKCA d-Cert CA 1 - 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 CA 1 - 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=[Authorised Unit name] (Note 1) e=[email address] (Note 2) ou=[SRN] (Note 3) ou=[BRN+CI/CR+Others] (Note 4) ou=[Subscriber Organisation Name] (Note 5) ou=[Subscriber Organisation branch/dept] (Note 5) o=HKCA d-Cert (Encipherment) c=HK
Subject public key info		Algorithm ID: RSA Public Key: 2048-bit key size
Issuer unique identifier		Not used
Subject unique identifier		Not used
Standard extension (Note 6)		
Authority Key Identifier		[Subject Key Identifier of the issuer's certificate]
Key usage		Digital Signature, Key Encipherment **(This field will be set Critical.)**
Certificate policies		Policy Identifier = [OID] (Note 7) Policy Qualifier Id = CPS Qualifier : [URL of CPS]
Subject alternative name	**DNS**	Not used
	Rfc822	[email address] (Note 2)
Issuer alternative name		Not used
Basic constraints	**Subject type**	End Entity
	Path length constraint	None
Extended key usage		SSL Client, S/MIME
CRL distribution points		Distribution Point Name = [URL of CRL Distribution Point] (Note 8)
Netscape extension (Note 6)		
Netscape cert type		Not used
Netscape SSL server name		Not used
Netscape comment		Not used

Note

1. Name of the Authorised Unit of the Subscriber Organisation.
2. Email address provided by the Authorised Representative
3. SRN: 10-digit Subscriber Reference Number
4. Business Registration Certificate Number (BRN): a string of 16 digits/alphabets [filled with all zeroes if BRN is not available]. Certificate of Incorporation (CI)/ Certificate of Registration (CR): a string of 8

digits/alphabets [filled with leading zeros if CI/CR is shorter than 8 digits/alphabets, all zeroes if CI/CR is not available, or all zeros for Limited Partnership Fund (LPF)]. Others: a string of max. 30 digits/alphabets (blank if null). For HKSAR government departments, BRN and CI/CR are filled with zeroes, department name in abbreviation (e.g. DPO for Digital Policy Office) is placed in Others. For an organisation who is registered as an LPF under the Limited Partnership Fund Ordinance (Cap. 637), the respective CR is placed in Others.

5. 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, their company names will not be included in this field (see Section 3.1.1.6 of this CPS).

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

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

8. URL of CRL Distribution Point is http://crl.hkca.hk/crl/HKCAdCertCA1-25CRL_<xxxxx>.crl which are partitioned CRLs issued by the Sub CA “HKCA d-Cert CA 1 - 25”, where <xxxxx> is a string of five alphanumeric characters generated by the CA system. HKCA publishes several partitioned CRLs for this type of certificate. If a certificate is suspended or revoked, its information will be published in the partitioned CRL at the URL specified in this CRL Distribution Point field.

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

The Appendix C of this CPS provides the arrangement of updating and publishing the Certificate Revocation Lists (CRLs) issued by the Sub CAs "HKCA d-Cert CA 1 - 25", "HKCA d-Cert CA 1 - 25A", as well as the Authority Revocation Lists (ARLs) issued by the Root CA "HKCA Root CA 1". Additionally, it specifies the format of these CRLs and ARLs.

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

a) **Partitioned CRLs** that contain Information of suspended or revoked certificates in groups. Each of the partitioned CRLs is available for public access at the following locations (URLs):
   i. d-Cert (Personal), d-Cert (Organisational) and d-Cert (Encipherment) issued by Sub CA "HKCA d-Cert CA 1 - 25" :
      http://crl.hkca.hk/crl/HKCAdCertCA1-25CRL_<xxxxx>.crl
      where <xxxxx> is a string of five alphanumeric characters.
   ii. d-Cert (Personal) and d-Cert (Organisational) that supports Adobe PDF signing, issued by Sub CA "HKCA d-Cert CA 1 - 25A" :
      http://crl.hkca.hk/crl/HKCAdCertCA1-25ACRL_<xxxxx>.crl
      where <xxxxx> is a string of five alphanumeric characters.

b) **Full CRLs** that contain Information of all suspended or revoked certificates that are issued by the Sub CA "HKCA d-Cert CA 1 - 25" and "HKCA d-Cert CA 1 - 25A" respectively. Each of the full CRLs is available at the following locations (URLs):

   i. Certificates issued by Sub CA "HKCA d-Cert CA 1 - 25" :
      http://crl.hkca.hk/crl/HKCAdCertCA1-25CRL.crl or
      ldap://ldap.hkca.hk (port 389, cn=HKCA d-Cert CA 1 - 25 CRL, o=Hong Kong Internet Registration Corporation Limited, c=HK)
   ii. Certificates issued by Sub CA "HKCA d-Cert CA 1 - 25A" :
      http://crl.hkca.hk/crl/HKCAdCertCA1-25ACRL.crl or
      ldap://ldap.hkca.hk (port 389, cn=HKCA d-Cert CA 1 - 25A CRL, o=Hong Kong Internet Registration Corporation Limited, c=HK)

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

Under normal circumstances, HKCA will 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 website on ad hoc basis without prior notice.

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

i. Sub CA certificates issued by Root CA "HKCA Root CA 1":
http://crl.hkca.hk/crl/RootCA1ARL.crl or
ldap://ldap.hkca.hk (port 389, cn=HKCA Root CA 1 ARL, o=Hong Kong Internet Registration Corporation Limited, c=HK)

(I) Format of Partitioned and Full CRL issued by the Sub CA "HKCA d-Cert CA 1 - 25" under this CPS:

Standard Fields	Sub-fields	Field Contents of Partitioned CRL	Field Contents of Full CRL	Remarks
Version		v2		This field describes the version of encoded CRL as X.509 v2.
Signature algorithm ID		sha256RSA		This field contains the algorithm identifier for the algorithm used to sign the CRL.
Issuer name		cn=HKCA d-Cert CA 1 - 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 2)				
Authority Key Identifier		[Subject Key Identifier of the Sub CA issuing this CRL]		
CRL number		[Generated by CA system – each partitioned CRL has its own sequence]		The CRL Number is generated in sequence for each CRL issued by a CA.
Issuer distribution point		[DER Encoded CRL Distribution Point] **(This field will be set Critical.)**	Not used	This field is used for Partitioned CRLs only.

(II) Format of Partitioned and Full CRL issued by the Sub CA "HKCA d-Cert CA 1 - 25A" under this CPS:

Standard Fields	Sub-fields	Field Contents of Partitioned CRL	Field Contents of Full CRL	Remarks
Version		v2		This field describes the version of encoded CRL as X.509 v2.

Standard Fields	Sub-fields	Field Contents of Partitioned CRL	Field Contents of Full CRL	Remarks
Signature algorithm ID		sha256RSA		This field contains the algorithm identifier for the algorithm used to sign the CRL.
Issuer name		cn=HKCA d-Cert CA 1 - 25A, 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 2)				
Authority Key Identifier		[Subject Key Identifier of the Sub CA issuing this CRL]		
CRL number		[Generated by CA system – each partitioned CRL has its own sequence]		The CRL Number is generated in sequence for each CRL issued by a CA.
Issuer distribution point		[DER Encoded CRL Distribution Point] **(This field will be set Critical.)**	Not used	This field is used for Partitioned CRLs only.

(III) Format of ARL issued by the root CA "HKCA Root CA 1" under this CPS :

Standard Fields	Sub-fields	Field Contents of ARL	Remarks
Version		v2	This field describes the version of encoded ARL as X.509 v2.
Signature algorithm ID		sha256RSA	This field contains the algorithm identifier for the algorithm used to sign the ARL.
Issuer name		cn=HKCA Root CA 1 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.

Standard Fields	Sub-fields	Field Contents of ARL	Remarks
Next update		[UTC time]	"Next Update" contains the date by which the next ARL will be issued, but it will not be issued any later than the indicated date. Notwithstanding this, the ARL is updated and issued on an **annual** basis as stated in the CPS.
Revoked certificates	**User certificate**	[Certificate Serial Number]	Revoked certificates are listed by their serial numbers.
	Revocation date	[UTC time]	The date on which the revocation occurred is specified.
	CRL entry extensions		
	Reason code	[Revocation Reason Code]	(Note 1)
Standard extension (Note 2)			
Authority Key Identifier		[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.
Issuer distribution point		Only Contains User Certs=No Only Contains CA Certs=Yes Indirect CRL=No **(This field will be set Critical.)**	

Note

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

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

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

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

Appendix D - Summary of HKCA d-Cert Features

1) d-Cert (Personal) Certificate

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

2) d-Cert (Organisational) and d-Cert (Encipherment) Certificate

Features	d-Cert (Organisational) Certificates	d-Cert (Organisational) that supports Adobe PDF signing	d-Cert (Encipherment) Certificates
Subscribers	Organisations that hold a valid business registration certificate(Note 1) issued by the Government of the Hong Kong SAR, statutory bodies of Hong Kong whose existence is recognized by the laws of Hong Kong and bureaux, departments or agencies of Government of HKSAR		
Certificate Holders	Authorised Users who are members or employees of the Organisation as the Subscriber		Authorised Units of the Organisation as the Subscriber
Reliance Limit	HK$200,000		
Recognized Certificate	Yes		
Key pair size	2048-bit RSA		
Key pair generation	By HKCA on behalf of the Subscriber through the central key generation service.		
Identity verification	Authentication of the identity of the organisation and its Authorised Representative		
Usage of certificate	Digital Signature and Encryption		Encryption only
Subscriber's information included in the certificate	▪ Subscriber Organisation's name, including its Chinese name if provided ▪ Authorised User's name and email address ▪ Subscriber Reference Number (SRN) generated by the HKCA system ▪ Subscriber Organisation's company/business registration information(Note 2)		▪ Subscriber Organisation's name ▪ Authorised Unit's name and email address ▪ Subscriber Reference Number (SRN) generated by the HKCA system ▪ Subscriber Organisation's company/business registration information
Subscription Fees and Administration Fees	(see Section 2.4 of this CPS)		
Certificate Validity	One year or two years	One year or two years or three years	One year or two years or three years
	(see Sections 1.2.4 and 3.3.2 of this CPS)		

Note

1. For subscribers of d-Cert (Organisational), organisations that hold a valid certification letter issued by the Inland Revenue Department of the Government of Hong Kong SAR to Reporting Financial Institution / Reporting Entity as referred in Inland Revenue Ordinance (Cap. 112) are also acceptable (see Section 1.2.3.2).

2. For organisations that hold a valid certification letter issued by the Inland Revenue Department of the Government of Hong Kong SAR to Reporting Financial Institution / Reporting Entity as referred in Inland Revenue Ordinance (Cap. 112), only the IRD Reference Number of the certification letter will be included in the certificate.

Appendix E - List of Registration Authorities for the HKCA d-Cert

As of the effective date of this CPS, no Registration Authority for HKCA d-Cert is appointed.

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

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

Appendix G - Lifespan of CA root certificates

Name of the root certificate	Lifespan	Remarks
HKCA Root CA 1	20 October 2025 – 14 October 2050	
HKCA d-Cert CA 1 - 25	4 December 2025 – 30 November 2040	This Sub CA commences to issue d-Cert under this CPS to applicants with effect from [TBC].
HKCA d-Cert CA 1 - 25A	4 December 2025 – 30 November 2040	This Sub CA commences to issue d-Cert under this CPS to applicants with effect from [TBC].

Appendix H – List of Particular Applications and Corresponding Application-specific Codes for HKCA d-Cert

As of the effective date of this CPS, no application-specific codes is assigned to HKCA d-Cert.

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

Disclaimer: The comparison table provided below is intended for the convenience of cross-referencing between the RFC 3647 and this CPS. The provisions of this CPS will always prevail whenever contradiction in meaning arises between this CPS and the RFC 3647, and Subscriber or any relying party will not hold HKCA liable for loss and damage that they would sustain due to such contradiction or their reliance of the comparison table provided below.

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

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

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

Sections of RFC3647	Relevant sections of this CPS	Explanations
4.5.2 Relying Party Public Key and Certificate Usage	2.1.6	
4.6 Certificate Renewal	3.2	
4.6.1 Circumstances for Certificate Renewal	3.2	
4.6.2 Who May Request Renewal	3.2	
4.6.3 Processing Certificate Renewal Requests	3.2	
4.6.4 Notification of New Certificate Issuance to Subscriber	4.1 - 4.3	
4.6.5 Conduct Constituting Acceptance of a Renewal Certificate	4.1 - 4.3	
4.6.6 Publication of the Renewal Certificate by the CA	2.5 and 4.1 - 4.3	
4.6.7 Notification of Certificate Issuance by the CA to Other Entities	2.5 and 4.1 - 4.3	
4.7 Certificate Re-Key	3.2	Certificate Re-Key will take place during Certificate Renewal process.
4.7.1 Circumstances for Certificate Re-Key	3.2	
4.7.2 Who May Request Certification of a New Public Key	3.2	
4.7.3 Processing Certificate Re-Keying Requests	3.2	
4.7.4 Notification of New Certificate Issuance to Subscriber	4.1 - 4.3	
4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate	4.1 - 4.3	
4.7.6 Publication of the Re-Keyed Certificate by the CA	2.5 and 4.1 - 4.3	
4.7.7 Notification of Certificate Issuance by the CA to Other Entities	2.5 and 4.1 - 4.3	
4.8 Certificate Modification	Not Applicable	This CPS does not allow modification of an issued d-Cert.
4.8.1 Circumstances for Certificate Modification		
4.8.2 Who May Request Certificate Modification		
4.8.3 Processing Certificate Modification Requests		
4.8.4 Notification of New Certificate Issuance to Subscriber		
4.8.5 Conduct Constituting Acceptance of Modified Certificate		
4.8.6 Publication of the Modified Certificate by the CA		
4.8.7 Notification of Certificate Issuance by the CA to Other Entities		
4.9 Certificate Revocation and Suspension	4.5	
4.9.1 Circumstances for Revocation	2.1.4, 4.5.1 and 4.10.2	
4.9.2 Who Can Request Revocation	4.5.2	
4.9.3 Procedure for Revocation Request	4.5.2	
4.9.4 Revocation Request Grace Period	4.5.2	
4.9.5 Time Within Which CA Must Process the Revocation Request	4.5.3	
4.9.6 Revocation Checking Requirements for Relying Parties	2.1.6 and 4.5.3	
4.9.7 CRL Issuance Frequency	4.5.3 and 4.10.2	
4.9.8 Maximum Latency for CRLs	4.5.3	
4.9.9 On-Line Revocation/Status Checking Availability	Not Applicable	Online status checking is currently not provided.

Sections of RFC3647	Relevant sections of this CPS	Explanations
4.9.10 On-Line Revocation Checking Requirements	Not Applicable	Online status checking is currently not provided.
4.9.11 Other Forms of Revocation Advertisements Available	Not Applicable	Other forms of revocation advertisements are currently not provided.
4.9.12 Special Requirements re Key Compromise	Not Applicable	This service is currently not provided.
4.9.13 Circumstances for Suspension	2.1.4 and 4.5.2	
4.9.14 Who Can Request Suspension	4.5.2	
4.9.15 Procedure for Suspension Request	4.5.2	
4.9.16 Limits on Suspension Period	4.5.2	
4.10 Certificate Status Services	4.5.3 and 4.5.4	
4.10.1 Operational Characteristics	4.5.3	
4.10.2 Service Availability	4.5.3	
4.10.3 Operational Features	4.5.3	
4.11 End of Subscription	4.6	
4.12 Key Escrow and Recovery	6.2.3	
4.12.1 Key Escrow and Recovery Policy and Practices	6.2.3	
4.12.2 Session Key Encapsulation and Recovery Policy and Practices	6.2.3	
5. Facility, Management, and Operational Controls	2.1.4, 2.1.6, 4 and 5	
5.1 Physical Controls	5.1	
5.1.1 Site Location and Construction	5.1.1	
5.1.2 Physical Access	5.1.2	
5.1.3 Power and Air Conditioning	5.1.4	
5.1.4 Water Exposures	5.1.5	
5.1.5 Fire Prevention and Protection	5.1.6	
5.1.6 Media Storage	5.1.7	
5.1.7 Waste Disposal	5.1.10	
5.1.8 Off-site Backup	5.1.8	
5.2 Procedural Controls	5.2	
5.2.1 Trusted Roles	5.2.1	
5.2.2 Number of Personnel Needed for Each Task	5.2.1	
5.2.3 Identification and Authentication of Each Role	5.2.1	
5.2.4 Roles requiring Segregation of Duties	5.2.1	
5.3 Personnel Controls	5.3	
5.3.1 Qualifications, Experience, and Clearance Requirements	5.3.1	
5.3.2 Background Check Procedures	5.3.2	
5.3.3 Training Requirements	5.3.3	
5.3.4 Retraining Frequency and Requirements	5.3.3	

Sections of RFC3647	Relevant sections of this CPS	Explanations
5.3.5 Job Rotation Frequency and Sequence	Non-disclosure	This CPS does not disclose the contents of this section in accordance with the internal policy.
5.3.6 Sanctions for Unauthorised Actions	5.3.4	
5.3.7 Independent Contractor Requirements	Non-disclosure	This CPS does not disclose the contents of this section in accordance with the internal policy.
5.3.8 Documentation Supplied to Personnel	5.3.5	
5.4 Audit Logging Procedures	4.7	
5.4.1 Types of Events Recorded	4.7.1	
5.4.2 Frequency of Processing Log	4.7.2	
5.4.3 Retention Period for Audit Log	4.7.3	
5.4.4 Protection of Audit Log	4.7.4	
5.4.5 Audit Log Backup Procedures	4.7.5	
5.4.6 Audit Collection System (Internal vs. External)	4.7.6	
5.4.7 Notification to Event-Causing Subject	4.7.7	
5.4.8 Vulnerability Assessments	4.7.8	
5.5 Records Archival	4.8	
5.5.1 Types of Records Archived	4.8.1	
5.5.2 Retention Period for Archive	4.8.2	
5.5.3 Protection of Archive	4.8.3	
5.5.4 Archive Backup Procedures	4.8.4	
5.5.5 Requirements for Time-Stamping of Records	4.8.5	
5.5.6 Archive Collection System (Internal or External)	4.8.4	
5.5.7 Procedures to Obtain and Verify Archive Information	4.8.4	
5.6 Key Changeover	4.9	
5.7 Compromise and Disaster Recovery	4.10	
5.7.1 Incident and Compromise Handling Procedures	4.10	
5.7.2 Computing Resources, Software, and/or Data Are Corrupted	4.10.4	
5.7.3 Entity Private Key Compromise Procedures	4.10.2	
5.7.4 Business Continuity Capabilities After a Disaster	4.10.1	
5.8 CA or RA Termination	4.11 and 4.12	
6. Technical Security Controls	6	
6.1 Key Pair Generation and Installation	6.1	
6.1.1 Key Pair Generation	6.1.1 and 6.1.5	
6.1.2 Private Key Delivery to Subscriber	6.1.3	
6.1.3 Public Key Delivery to Certificate Issuer	6.1.2	
6.1.4 CA Public Key Delivery to Relying Parties	4.1 - 4.4	

Sections of RFC3647	Relevant sections of this CPS	Explanations
6.1.5 Key Sizes	6.1.4	
6.1.6 Public Key Parameters Generation and Quality Checking	6.1.5	
6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)	6.1.6	
6.2 Private Key Protection and Cryptographic Module Engineering Controls	6.2 and 6.7	
6.2.1 Cryptographic Module Standards and Controls	6.2.1 and 6.7	
6.2.2 Private Key (n out of m) Multi-Person Control	6.2.2	
6.2.3 Private Key Escrow	6.2.3	
6.2.4 Private Key Backup	6.2.4	
6.2.5 Private Key Archival	Non-disclosure	This CPS does not disclose the contents of this section in accordance with the internal policy.
6.2.6 Private Key Transfer between Cryptographic Modules	6.2.5	
6.2.7 Private Key Storage on Cryptographic Module	6.2.5	
6.2.8 Method of Activating Private Key	6.2.4	
6.2.9 Method of Deactivating Private Key	6.2.2	
6.2.10 Method of Destroying Private Key	Non-disclosure	This CPS does not disclose the contents of this section in accordance with the internal policy.
6.2.11 Cryptographic Module Rating	6.2.1 and 6.7	
6.3 Other Aspects of Key Pair Management	6.3	
6.3.1 Public Key Archival	6.3	
6.3.2 Certificate Operational Periods and Key Pair Usage Periods	6.3	
6.4 Activation Data	6.1 and 6.2	
6.4.1 Activation Data Generation and Installation		
6.4.2 Activation Data Protection		
6.4.3 Other Aspects of Activation Data		
6.5 Computer Security Controls	6.4	
6.5.1 Specific Computer Security Technical Requirements	6.4	
6.5.2 Computer Security Rating	6.4	
6.6 Life Cycle Technical Controls	6.5	
6.6.1 System Development Controls	6.5	
6.6.2 Security Management Controls	6.5	
6.6.3 Life Cycle Security Controls	6.5	
6.7 Network Security Controls	6.6	
6.8 Time-Stamping	Not Applicable	Not provided
7. Certificate, CRL, and OCSP Profiles	7	
7.1 Certificate Profile	7.1	

Sections of RFC3647	Relevant sections of this CPS	Explanations
7.1.1 Version Number(s)	Appendix B	
7.1.2 Certificate Extensions	Appendix B	
7.1.3 Algorithm Object Identifiers	Appendix B	
7.1.4 Name Forms	Appendix B	
7.1.5 Name Constraints	Appendix B	
7.1.6 Certificate Policy Object Identifier	Appendix B	
7.1.7 Usage of Policy Constraints Extension	Appendix B	
7.1.8 Policy Qualifiers Syntax and Semantics	Appendix B	
7.1.9 Processing Semantics for the Critical Certificate Policies Extension	Appendix B	
7.2 CRL Profile	7.2	
7.2.1 Version Number(s)	Appendix C	
7.2.2 CRL and CRL Entry Extensions	Appendix C	
7.3 OCSP Profile	Not Applicable	Not provided
7.3.1 Version Number(s)	Not Applicable	
7.3.2 OCSP Extensions	Not Applicable	
8. Compliance Audit and Other Assessments	2.6	
8.1 Frequency and Circumstances of Assessment	2.6	
8.2 Identity/Qualifications of Assessor	2.6	
8.3 Assessor's Relationship to Assessed Entity	2.6	
8.4 Topics Covered by Assessment	2.6	
8.5 Actions Taken as a Result of Deficiency	Non-disclosure	This CPS does not disclose the contents of this section in accordance with the internal policy.
8.6 Communications of Results	Non-disclosure	This CPS does not disclose the contents of this section in accordance with the internal policy.
9. Other Business and Legal Matters	2	
9.1 Fees	2.4	
9.1.1 Certificate Issuance or Renewal Fees	2.4	
9.1.2 Certificate Access Fees	2.4	
9.1.3 Revocation or Status Information Access Fees	2.4	
9.1.4 Fees for Other Services	2.4	
9.1.5 Refund Policy	2.4	
9.2 Financial Responsibility	2.2.15	
9.2.1 Insurance Coverage	2.2.15	
9.2.2 Other Assets	2.2.15	
9.2.3 Insurance or Warranty Coverage for End-Entities	2.2.15	
9.3 Confidentiality of Business Information	2.7	

Sections of RFC3647	Relevant sections of this CPS	Explanations
9.3.1 Scope of Confidential Information	2.7	
9.3.2 Information Not Within the Scope of Confidential Information	2.7	
9.3.3 Responsibility to Protect Confidential Information	2.7	
9.4 Privacy of Personal Information	2.7	
9.4.1 Privacy Plan	2.7	
9.4.2 Information Treated as Private	2.7	
9.4.3 Information Not Deemed Private	2.7	
9.4.4 Responsibility to Protect Private Information	2.7	
9.4.5 Notice and Consent to Use Private Information	Not Applicable	This CPS does not disclose the contents of this section in accordance with RFC2527.
9.4.6 Disclosure pursuant to judicial or administrative process	2.7	
9.4.7 Other Information Disclosure Circumstances	2.7	
9.5 Intellectual Property rights	1.2.2.1	
9.6 Representations and Warranties	2	
9.6.1 CA Representations and Warranties	2.2.3	
9.6.2 RA Representations and Warranties	2.1.1	
9.6.3 Subscriber Representations and Warranties	2.1.4	
9.6.4 Relying Party Representations and Warranties	2.1.6	
9.6.5 Representations and Warranties of Other Participants	Not Applicable	This CPS does not disclose the contents of this section in accordance with RFC2527.
9.7 Disclaimers of Warranties	2.2.10	
9.8 Limitations of Liability	2.2.3	
9.9 Indemnities	2.2.3	
9.10 Term and Termination	Not Applicable	Currently not defined
9.10.1 Term		
9.10.2 Termination		
9.10.3 Effect of Termination and Survival		
9.11 Individual Notices and Communications with Participants	2.1.1	
9.12 Amendments	8	
9.12.1 Procedure for Amendment	8	
9.12.2 Notification Mechanism and Period	8	
9.12.3 Circumstances Under Which OID Must be Changed	8	
9.13 Dispute Resolution Provisions	2.3.3	
9.14 Governing Law	2.3.1	
9.15 Compliance with Applicable Law	2.3.1	
9.16 Miscellaneous Provisions	2.3	

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