THE CERTIFICATION PRACTICE STATEMENT

OF

THE HONG KONG INTERNET REGISTRATION CORPORATION LIMITED

As

A Recognized Certification Authority
under the Electronic Transactions Ordinance

for

HKCA iAM Smart-Cert

Date : [TBC]
OID : 1.3.6.1.4.1.64092.1.9.1

Table of Contents

PREAMBLE

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

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

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

Under the Ordinance, 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 has decided so to pursue recognition as a Recognized CA and is referred to in this document as **HKIRC** or **HKCA**.

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.

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, 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 iAM Smart-Certs issued under this Certification Practice Statement ("CPS") are Recognized Certificates under the Ordinance and are referred to as "Certificates" (upper or lower case) or "iAM Smart-Certs" in this CPS.**

This CPS sets out practices and standards for iAM Smart-Certs, and the structure of this CPS is as follows:

Section 1 provides an overview and contact details
Section 2 sets out the functions and obligations of the parties
Section 3 sets out identification and authentication requirements

Section 4 describes the operational requirements
Section 5 describes the security controls
Section 6 sets out how the Key Pairs will be generated and controlled
Section 7 describes the certificate, Certificate Revocation List and Online Certificate Status Protocol profiles
Section 8 documents how this CPS will be administered
Section 9 sets out other business and legal matters

Appendix A contains a glossary
Appendix B contains a HKCA iAM Smart-Cert format
Appendix C contains a HKCA Certificate Revocation List format
Appendix D contains a summary of HKCA iAM Smart-Cert features
Appendix E describes lifespan of CA root certificates

1. INTRODUCTION

1.1 Overview

This CPS is published for public knowledge by HKCA and specifies the practices and standards that HKCA employs in issuing iAM Smart-Certs.

The Internet Assigned Numbers Authority ("IANA") has assigned the Private Enterprise Number 64092 to HKCA. For identification purpose, this CPS bears an Object Identifier ("OID") "1.3.6.1.4.1.64092.1.9.1" (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 for the issuance, revocation and publication of iAM Smart-Certs. 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.

One of the digital infrastructure projects announced in October 2017 was the provision of electronic identity to Hong Kong residents free of charge. The Government has launched the relevant digital infrastructure which is officially be named as "iAM Smart" platform. "iAM Smart" is a digital identity provided for all Hong Kong residents, enabling them to use a single digital identity and authentication to conduct government and commercial transactions online.

iAM Smart can be obtained by Hong Kong residents using different registration channels which provide different versions of iAM Smart. Only holders of iAM Smart registered in accordance with Section 3.1.1 are eligible for applying an iAM Smart-Cert.

iAM Smart-Certs issued by HKCA in accordance with this CPS are specifically designated for the Subscribers who are holders of iAM Smart registered in accordance with Section 3.1.1 to conduct digital signing with legal backing under the Ordinance. Unless otherwise specified, the iAM Smart version mentioned in ensuing sections of this CPS refers to the version of iAM Smart obtained in accordance with Section 3.1.1 and is referred as iAM Smart in this CPS.

Under the Ordinance, HKCA is a Recognized CA. **HKCA has designated the iAM Smart-Certs issued under this CPS as Recognized Certificates**. As the iAM Smart-Cert enjoys the status as a Recognized Certificate under the Ordinance, electronic transactions in which an iAM Smart-Cert is used for digital signing shall be given recognition and protection as stated in the Ordinance.

iAM Smart-Cert adopts a PKI model wherein a Subscriber remotely accesses the Private Key on a hardware security module ("HSM") hosted in the iAM Smart System. The Subscriber's Key Pair for iAM Smart-Cert is generated in the HSM and the Private Key is stored in the HSM once generated.

A summary of the iAM Smart-Cert features is in **Appendix D**.

1.2 Community and Applicability

1.2.1 Certification Authority

Under this CPS, HKCA performs the functions of a CA. HKCA is the only CA authorised to issue iAM Smart-Cert under this CPS (see Section 2.1.1).

1.2.1.1 Effect

HKCA publishes iAM Smart-Certs in a Repository.

1.2.1.2 HKCA's Right to Subcontract

HKCA may appoint agents or subcontractors to perform some or all of the functions stated in this CPS and the Subscriber Agreement. Regardless of any such appointment, HKCA shall remain

as, and perform the role of, the CA and the issuer of the iAM Smart-Certs.

1.2.2 iAM Smart Registration Office ("iAMSmartRO")

HKCA mostly deals with the Applicant or Subscriber of iAM Smart-Cert via iAMSmartRO. DPO performs the functions of iAMSmartRO and may appoint contractor(s) to perform some or all of the functions of the iAMSmartRO. iAMSmartRO is the Registration Authority acting on behalf of HKCA in performing the following functions:
a) receipt and processing of certificate application from the Applicant and Subscriber;
b) verification of the identity of the Applicant and Subscriber;
c) retention of copies of the documentary evidence that identifies the Applicant and Subscriber; and
d) notification to the Applicant and the Subscriber on approval or rejection of certificate application and on revocation of certificate.

All functions to be performed by iAMSmartRO are set out in Section 2.1.2 below.

1.2.3 End Entities

Under this CPS there are two types of end entities, Subscribers and Relying Parties.

NOTE TO RELYING PARTIES: A person under 18 years of age may also follow Sections 3 and 4 of this CPS to apply for an iAM Smart-Cert.

1.2.3.1 Location of the Private Key

An iAM Smart-Cert Private Key will be stored in a HSM hosted in the iAM Smart System. HKCA will publish the certificate (with Public Key) in the Repository, for the public to download and for the purpose of verification of Digital Signatures.

1.2.3.2 Subscriber and the iAMSmartRO

Subscriber must authorise the iAMSmartRO to keep custody and manage the Private Key and keep a copy of iAM Smart-Cert issued by HKCA to the Subscriber. Subscriber acknowledges that the iAMSmartRO may also at the same time act on behalf of HKCA for performing the functions stated in Section 1.2.2 above. Subscriber acknowledges and agrees that there is no conflict arising from such functions carried out by the iAMSmartRO, and it is beneficial to all parties that the iAMSmartRO should take on such functions.

1.2.4 Class of Certificate

iAM Smart-Cert is the only class of certificate that may be issued by HKCA under this CPS. HKCA issues iAM Smart-Cert only to Applicants who have confirmed their acceptance of a Subscriber Agreement in the form specified by HKCA, and their identity successfully verified and application accepted by the iAMSmartRO in accordance with Sections 3 and 4 of this CPS. It may be used by Subscribers via the iAM Smart System to perform government and commercial transactions with the Relying Parties that accept Digital Signature by iAM Smart-Cert.

iAM Smart-Cert may be issued to persons under 18 years of age (see also Section 3.1.3).

1.2.5 Certificate Lifespan

The validity period of an iAM Smart-Cert issued under this CPS is 1 year, commencing on the date the iAM Smart-Cert is issued by HKCA.

1.2.6 Application

All first applications and renewal applications of iAM Smart-Cert will require the Applicants to fulfil the requirements as described in Sections 3 and 4 of this CPS.

1.2.7 Applicability

An iAM Smart-Cert issued to a Subscriber is for general purpose use. It is not restricted to any specific type of transaction.

1.3 Contact Details

Applicants or Subscribers may send their enquiries, suggestions or complaints on iAM Smart-Cert 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 working days. In the cases where full replies cannot be issued within 10 working 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 Functions and Obligations

HKCA's functions are defined and limited by this CPS and by the terms of the contracts with Subscribers in the form of a Subscriber Agreement.

2.1.1 CA Functions and Obligations

In accordance with this CPS, HKCA performs the following functions (all or any of which may be performed by the iAMSmartRO or the Contractor under the management and control of HKCA):

a) Receive applications for iAM Smart-Cert via the iAMSmartRO;
b) Notify Applicants, via the iAMSmartRO, the approval or rejection of their applications;
c) Issue and publish iAM Smart-Certs in the Repository based on the CSR submitted by the iAMSmartRO;
d) Revoke iAM Smart-Certs and publish revised Certificate Revocation Lists ("CRLs") in a timely manner;
e) Provide Online Certificate Status Protocol ("OCSP") response for checking the status of iAM Smart-Cert;
f) Notify Subscribers, via the iAMSmartRO, the revocation of their iAM Smart-Cert.

HKCA is responsible under the Ordinance for the use of a Trustworthy System in performing its services (a) to issue or revoke an iAM Smart-Cert; or (b) to publish in a Repository or give notice of the issue or revocation of an iAM Smart-Cert.

2.1.2 iAMSmartRO Functions and Obligations

iAMSmartRO performs the following functions (all or any of the functions may be performed by a contractor under the management and control of iAMSmartRO):

<u>RA functions acting on behalf of HKCA (see Section 1.2.2)</u>

a) Receive and process certificate applications from the Applicant who must be a holder of iAM Smart (see Section 3.1.1);

b) Verify the identity of the Applicant / Subscriber both in first time application and renewal of iAM Smart-Cert (see Sections 3.1.2 and 3.2.1), and logging identity verification result in the iAM Smart System;

c) Verify the identity of Subscriber in any request for revocation of iAM Smart-Cert;

d) Keep all records of identity verification of Applicants as a holder of iAM Smart in accordance with the terms of this CPS and the Subscriber Agreement throughout the validity and for at least 7 years after expiry of the relevant certificate;

e) Notify the Applicant / Subscriber on approval or rejection of certification application and revocation of certificate upon receiving the notification from HKCA;

f) Inform the Subscriber of his obligations, including his duty to safeguard the iAM Smart credentials for accessing the iAM Smart-Cert via the iAM Smart System and to immediately report any compromise or suspected compromise to iAMSmartRO via the iAM Smart System or other communication channels to be designated by the iAMSmartRO;

<u>Other functions</u>

g) Submit certificate request to HKCA upon Applicant's confirmation of his acceptance of the terms and conditions of the Subscriber Agreement;

h) Generate the Subscriber's Key Pair and store the Private Key in the HSM of the iAM Smart System;

i) Keep custody of the Subscriber's Private Key and ensure that only the Subscriber can make use of his own Private Key to generate Digital Signature;

j) Ensure that when an iAM Smart-Cert is expired or with revocation status as shown in Repository, CRL or OCSP response, the Private Key of iAM Smart-Cert can no longer be used by its Subscriber or any other person;

k) Generate and submit the CSR to HKCA containing the Applicant related data and the Applicant's confirmation of his acceptance of the terms and conditions of the Subscriber Agreement.

The iAMSmartRO is responsible for the use of a Trustworthy System to deliver the above functions.

HKCA is and remains responsible for the activities of iAMSmartRO in the performance or purported performance by it of the above functions involving CA obligations and duties. iAMSmartRO only carries out on HKCA's behalf HKCA's obligations and duties in the RA functions.

2.1.3 Contractor Functions and 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 Obligations of Applicant and Subscriber

2.1.4.1 Applicant Obligations

Without prejudice to his other obligations as stated in this CPS and the Subscriber Agreement, an Applicant is responsible for all of the following:

a) Completing the application procedures properly through the iAM Smart System and ensuring accuracy of the representations and warranties made in the certificate application;

b) Confirming acceptance of a Subscriber Agreement in the form specified by HKCA and performing the obligations placed upon them by that Subscriber Agreement;

c) Agreeing that the iAM Smart System will, upon receiving the Applicant's iAM Smart-Cert application, generate the CSR to HKCA containing information in relation to the Applicant together with the Applicant's confirmation of his acceptance of the terms and conditions of the Subscriber Agreement;

d) Acknowledging that by submitting an iAM Smart-Cert application, he agrees that the receipt of an issued iAM Smart-Cert by the iAM Smart System is to be regarded as the Applicant's Acceptance of the certificate, and authorises the publication of the iAM Smart-Cert to any other person or in the HKCA's Repository.

2.1.4.2 Subscriber Obligations

Without prejudice to his other obligations as stated in this CPS and the Subscriber Agreement, a Subscriber is responsible for all of the following:

a) Agreeing that the Subscriber's Key Pair is generated and the Private Key is to be kept by the iAMSmartRO via the iAM Smart System in a HSM and an environment within the iAMSmartRO's premises;

b) Following the requirements specified in this CPS concerning the application for first time issue and renewal of certificates;

c) Notifying the iAMSmartRO from time to time of any change in the information in the certificate provided by the Subscriber;

d) Notifying the iAMSmartRO immediately of any occurrence of event which may entitle HKCA, upon the grounds set out in Section 4.2 below, to revoke the certificate;

e) Agreeing that by having been issued a certificate he warrants and represents to HKCA and to all Relying Parties that during the validity period of the certificate, the warranties and representations stated in Section 9.6.2 are and will remain true, accurate and complete;

f) Not using a certificate in a transaction on becoming aware of any ground upon which HKCA could revoke the certificate under the terms of this CPS, or after the Subscriber has made a revocation request or has received from HKCA a Revocation Notice under Section 4.2;

g) Upon becoming so aware of any ground upon which HKCA could revoke the certificate, or upon he himself has made a revocation request or upon having received from HKCA a Revocation Notice under Section 4.2, immediately notifying the 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 his own 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.

2.1.5 Relying Party Obligations

Without prejudice to its other obligations as stated in this CPS and the Subscriber Agreement, a Relying Party relying upon an iAM Smart-Cert is responsible for all of the following:

a) Relying on iAM Smart-Cert only when the reliance is reasonable and in good faith in light of all the circumstances known to the Relying Party at the time of the reliance;
b) Before relying upon an iAM Smart-Cert determining that the use of the iAM Smart-Cert and any Digital Signature supported by it is appropriate for its purposes;
c) Performing all acts as specified in Section 9.6.3.

2.2 Subscription Fees

iAM Smart-Cert is provided to the Subscriber for free.

2.3 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 iAM Smart-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

2.3.1 Certificate Repository Controls

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

2.3.2 Certificate Repository Access Requirements

Only persons authorised by HKCA have access to the Repository to update and modify the contents.

2.3.3 Certificate Repository Update

The Repository is updated promptly after the receipt by the iAM Smart System of the iAM Smart-Cert issued by HKCA or the receipt by HKCA of CRL update request from the Applicant via iAMSmartRO.

2.3.4 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.

2.4 Compliance Assessment

Compliance assessments conducted on the HKCA's system of issuing, revoking, suspending and publishing iAM Smart-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.

3. IDENTIFICATION AND AUTHENTICATION REQUIREMENTS

3.1 First Time Application

3.1.1 Holder of iAM Smart as Pre-requisite

iAM Smart can be obtained by Hong Kong residents using different registration channels. Only holders of iAM Smart (i) registered at iAM Smart Registration Points or (ii) registered through iAM Smart mobile app on smartphone equipped with Near Field Communication (NFC) function are eligible for applying an iAM Smart-Cert.

Hong Kong residents can obtain iAM Smart at iAM Smart Registration Points upon successful in-person identity verification by iAMSmartRO by providing HKID Card. They may visit the iAM Smart Registration Points and register through the designated devices equipped with a card reader which can identify the genuineness of the HKID Card and read the identity information (including English name, Chinese name (if available), HKID Card number and date of issue, date of birth and gender) in the HKID Card chip. If the designated device is not equipped with a card reader, personnel at the iAM Smart Registration Points shall verify the genuineness of the HKID Card and input the registrant's identity information into the iAM Smart System. The identity information and the live photo, if taken at the iAM Smart Registration Points, will be passed to the supporting IT system of the Immigration Department for HKID Card record checking to confirm if the registrant is a Hong Kong resident, if the identity information is valid and if the live photo matches the record in the Immigration Department. If live photo is not taken, personnel at the iAM Smart Registration Points shall review face-to-face the registrant's HKID Card and certify the photo printed on the HKID Card matches with the registrant's face.

Alternatively, Hong Kong residents may obtain iAM Smart by registration through the iAM Smart mobile app with a smartphone equipped with NFC function. The registrant will be asked to take a photo of his/her own HKID card for verification. Upon completion of the initial verification process, the iAM Smart mobile app will read the encrypted identity information (including English name, Chinese name (if available), HKID Card number and date of issue, date of birth and gender) from the HKID Card chip via NFC and pass them to the iAM Smart backend system where the encrypted identity information will be decrypted. The decrypted identity information and the registrant's selfie will be passed to the supporting IT system of the Immigration Department for HKID Card record checking so as to confirm if the registrant is a Hong Kong resident, whether the identity information is valid and the registrant's selfie matches the record in the Immigration Department.

3.1.2 Initial Application

Applicants for iAM Smart-Cert must submit applications via the iAM Smart System. An Applicant for iAM Smart-Cert must be a holder of iAM Smart (see Section 3.1.1). iAMSmartRO and its contractor will verify the identity of the Applicant as a holder of iAM Smart (i) via two-factor authentication procedures of the iAM Smart System or (ii) during the Applicant's registration of iAM Smart either at iAM Smart Registration Points or through iAM Smart mobile app on smartphone equipped with NFC, and the identity is verified upon successful registration of iAM Smart (see Section 3.1.1). Upon completion of identity verification, iAMSmartRO will submit the certificate application to HKCA.

HKCA will issue the iAM Smart-Cert to the successful Applicant via the iAM Smart System. The receipt of the issued certificate by the iAM Smart System will be regarded as the Applicant's Acceptance of the certificate.

3.1.3 Subscriber's Name appearing on the iAM Smart-Cert

The Subscriber for an iAM Smart-Cert is identified in the certificate with a Subject Name consisting of the Subscriber's name as verified in accordance with the procedures in Section 4.1. The

Subscriber's HKID Card number will be stored in the certificate as a hash value (see **Appendix B**).

For iAM Smart-Cert issued to a Subscriber who is under 18, the Subscriber is identified in the certificate with a Subject Name as specified above and the wording "iAM Smart-Cert (Minor)" (**see Appendix B**) to indicate that the Subscriber is under 18 at the time the iAM Smart-Cert is issued.

3.1.4 Method to Prove Authority to use the Private Key

The iAMSmartRO carries out the Digital Signature generation through the use of the Subscriber's Private Key. The Subscriber's Private Key is stored in the HSM hosted in the iAM Smart System. The Subscriber is required to pass through strong authentication procedures (viz., two-factor authentication procedures) for the authentication of his identity as a holder of iAM Smart as stipulated by the iAMSmartRO before he may invoke the use of the Private Key for the generation of Digital Signature.

The authorised personnel of iAMSmartRO is required to pass through strong authentication method designed by the iAMSmartRO before it may configure, operate and maintain the iAM Smart System storing the Private Key kept by the iAMSmartRO.

3.2 Certificate Renewal

3.2.1 Renewal of iAM Smart-Cert

The iAMSmartRO will notify the Subscribers to renew their certificates at least one month prior to the expiry of the certificates' validity period. The renewal procedures are as follows:-

(a) iAMSmartRO submits a renewal notification to the Subscriber by electronic means;
(b) Subscriber agrees to authorise iAMSmartRO to renew iAM Smart-Cert and authenticate his identity as a holder of iAM Smart via two-factor authentication procedures of the iAM Smart System;
(c) Subscriber submits the renewal application to HKCA via the iAM Smart System.

HKCA will not perform renewal of expired or revoked certificates.

3.2.2 Expired and Revoked iAM Smart-Cert

HKCA keeps publishing information of all expired and revoked certificates in the Repository with an annotation about their expiry or revocation status. Certificates which have been revoked are also published in CRL.

The time for updating the CRL for noting an iAM Smart-Cert with revocation status is specified in Section 4.2.3(a) below. As for the time for updating the Repository for noting an iAM Smart-Cert with expiry status, HKCA will update the expiry status on the Repository on the date of expiry. HKCA also provides OCSP response for checking the revocation status of iAM Smart-Cert.

Before allowing a Subscriber to use an iAM Smart-Cert, iAMSmartRO will check the validity period of the Subscriber's iAM Smart-Cert whether the iAM Smart-Cert is expired and check OCSP response, or CRL when OCSP is not available, whether the iAM Smart-Cert is revoked. It is incumbent on the iAMSmartRO to do the aforesaid verification to ensure that where an iAM Smart-Cert has expired or revoked, such iAM Smart-Cert can no longer be used by its Subscriber or any other person.

3.2.3 Periodic Review

The iAM Smart System will conduct periodic checking on the validity of the Subscriber's iAM Smart at least once a month by checking on the Subscriber's:

(a) deceased indicator;
(b) Hong Kong resident status;
(c) personal particulars (including English name, Chinese name (if available), HKID Card number, date of birth and gender) as shown on HKID Card; and
(d) status as iAM Smart holder.

If the periodic checking reveals that a Subscriber's iAM Smart becomes invalid because the Subscriber is dead or has lost his Hong Kong resident status or has changed his personal particulars under Section 3.2.3(c), iAMSmartRO will invalidate the Subscriber's iAM Smart and will notify HKCA to revoke the Subscriber's iAM Smart-Cert, after satisfying the notification requirements under Section 30(5) of Personal Data (Privacy) Ordinance (Cap. 486). HKCA will revoke the iAM Smart-Cert and iAMSmartRO will notify the Subscriber immediately after the revocation.

If the periodic checking reveals that a Subscriber is no longer a holder of iAM Smart under Section 3.2.3(d), iAMSmartRO will notify HKCA to revoke the iAM Smart-Cert and notify the Subscriber immediately after the revocation.

The Subscriber whose iAM Smart-Cert has been revoked may apply for a new iAM Smart-Cert if he is still eligible for it.

4. OPERATIONAL REQUIREMENTS

Unless otherwise specified, all provisions in this Section 4.1 apply to the application and issuance of iAM Smart-Cert.

4.1 Certificate Application, Issuance and Publication

4.1.1 Certificate Application

4.1.1.1 Applicant for iAM Smart-Cert at first time application must be a holder of iAM Smart (see Section 3.1.1), and must submit a request for certificate and accept the terms and conditions of the Subscriber Agreement via the iAM Smart System.

4.1.1.2 A Hong Kong resident will only be issued with iAM Smart after his identity information (including English name, Chinese name (if available), HKID Card number and date of issue, date of birth, gender, and resident status) is verified by iAMSmartRO (see Section 3.1.1). An Applicant for iAM Smart-Cert must be a holder of iAM Smart (see Section 3.1.1). The iAMSmartRO verifies on behalf of HKCA the identity of an Applicant by ensuring that the Applicant is a holder of iAM Smart (i) via the two-factor authentication procedures of the iAM Smart System or (ii) during the Applicant's registration of iAM Smart in accordance with Section 3.1.1, and the identity is verified upon successful registration of iAM Smart (see Section 3.1.1). Without prejudice to the representations set out in Section 40 of the Ordinance, no further verification will be conducted by HKCA concerning the Applicant's information and HKCA will receive the information, that is "the Applicant is a holder of iAM Smart and the identity information of the Applicant is verified by iAMSmartRO", on an as is basis.

4.1.2 Certificate Issuance

4.1.2.1 If identity verification as a holder of iAM Smart is successful, the iAMSmartRO will generate the Private Key and Public Key of the Applicant in a HSM hosted in the iAM Smart System and an environment within the iAMSmartRO's premises. The iAMSmartRO is responsible for ensuring that the Private Key will not be tampered with.

4.1.2.2 The iAMSmartRO will generate the CSR containing the Public Key in a Trustworthy System and environment within the iAMSmartRO's premises. The iAMSmartRO will prepare an interface file, containing the Applicant's data, the record of the Applicant's acceptance of the Subscriber Agreement and the CSR. The interface file, will be submitted electronically to HKCA.

4.1.2.3 Upon receipt of the CSR from the iAMSmartRO, HKCA will verify that the iAMSmartRO is in custody of the corresponding Private Key by checking the Digital Signature on the CSR structure with the contained Public Key. HKCA will not have possession of the Applicant's Private Keys.

4.1.2.4 Upon verifying the iAMSmartRO's custody of the corresponding Private Key, HKCA will generate the iAM Smart-Cert in which the Applicant's Public Key will be included. HKCA will then transmit the issued iAM Smart-Cert to the iAMSmartRO in a secure manner.

4.1.2.5 The iAMSmartRO will activate the iAM Smart-Cert by linking it to the Applicant's iAM Smart, and notify the Applicant via the iAM Smart System the application of iAM Smart-Cert is completed.

4.1.2.6 Acceptance of an iAM Smart-Cert by the Applicant is signified by the receipt of the iAM Smart-Cert by the iAM Smart System via which the Applicant submitted his iAM Smart-Cert application. Upon successful application and Acceptance of the iAM Smart-Cert, the Issued iAM Smart-Cert will be published in the Repository in accordance with Section 36 of the Ordinance.

4.1.2.7 The iAMSmartRO will keep custody of the Private Key upon receipt of the iAM Smart-Cert of the Applicant.

4.1.2.8 All application information transmitted electronically between iAMSmartRO and HKCA

must use a mutually agreed protocol.

4.1.3 Certificate Publication

HKCA will publish an iAM Smart-Cert in the Repository promptly after the issuance and Acceptance of that iAM Smart-Cert. Applicants can verify the information on the certificate through the Repository.

4.2 Certificate Revocation

4.2.1 Circumstances for Revocation

4.2.1.1 The compromise of a CA Private Key will result in prompt revocation of the certificates issued under that CA 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 CA Private Keys (see Section 4.6.2).

4.2.1.2 **Each Subscriber MUST immediately apply to HKCA (via the iAMSmartRO) for revocation of the certificate in accordance with the revocation procedures in this CPS where: the Subscriber's credential for accessing the iAM Smart has been, or is suspected of having been, compromised.**

4.2.1.3 **The iAMSmartRO MUST immediately notify and apply to HKCA for the revocation of an iAM Smart-Cert where: a Private Key, or the HSM containing the Private Key corresponding to the Public Key contained in that iAM Smart-Cert has been, or is suspected of having been, compromised. It must immediately notify the Subscriber(s) of the relevant iAM Smart-Cert(s) where the aforesaid notification and application for revocation relates to the iAM Smart-Cert issued to such Subscriber(s).**

4.2.1.4 HKCA will revoke an iAM Smart-Cert immediately by updating the certificate revocation list (CRL) and returning the revocation status through OCSP response, and by serving a notice to this effect to the Subscriber via the iAMSmartRO ("Revocation Notice") upon the occurrence of any of the events below in relation to such iAM Smart-Cert or if there is any suspicion of such occurrence:

a) the iAM Smart-Cert's Private Key has been compromised;
b) any information in the iAM Smart-Cert is not true or has become untrue or that the certificate is otherwise unreliable;
c) the iAM Smart-Cert was not properly issued in accordance with this CPS;
d) the Subscriber to whom the relevant iAM Smart-Cert was issued had failed to meet any of the obligations set out in this CPS or the Subscriber Agreement;
e) there is any regulation or law applicable to the certificate which requires such revocation;
f) the Subscriber's iAM Smart becomes invalid because the Subscriber to whom the iAM Smart-Cert was issued is dead or has lost his Hong Kong resident status or has change his personal particulars as shown on his HKID Card (see also Section 3.2.3(a)-(c));
g) the Subscriber has ceased to be a holder of iAM Smart (see also Section 3.2.3(d)); or
h) upon the Subscriber of iAM Smart-Cert (Minor) reaches age 18.

4.2.1.5 Where a Revocation Notice is served by HKCA on a Subscriber under Section 4.2.1.4, the iAMSmartRO must immediately cease the use of the Subscriber's iAM Smart-Cert and refrain from allowing the Private Key of the iAM Smart-Cert to be used.

4.2.2 Revocation Request Procedure

4.2.2.1 A Subscriber may submit a revocation request to HKCA via the iAMSmartRO through the iAM Smart System or other communication channels to be designated by iAMSmartRO. The

Subscriber should not submit a revocation request directly to HKCA.

4.2.2.2 The iAMSmartRO will, on behalf of HKCA, perform identity verification of the Subscriber where there is a revocation request from such Subscriber. The iAMSmartRO will forward the revocation request to HKCA immediately after verifying the identity of the Subscriber.

4.2.2.3 HKCA will immediately revoke the certificate after receiving the revocation request from iAMSmartRO.

4.2.2.4 The information of all certificates that have been revoked, including the reason code identifying the reason for the certificate revocation, will be included in the CRL (see Section 7.2) and could be checked by OCSP response (see Section 7.3).

4.2.3 Service Pledge & Certificate Revocation List (CRL) Update

a) HKCA will exercise reasonable endeavours to ensure that it will post the revocation status on the CRL after (1) actual receipt of a revocation request from the Subscriber via the iAMSmartRO under Section 4.2.2, or (2) the issuance of a Revocation Notice by HKCA under Section 4.2.1.4. However, the CRL is not immediately published in the directory for access by the public following each certificate revocation. Only when the next CRL is updated and published will it reflect the revoked status of the certificate. CRL is updated and published daily at 0915, 1415 and 1900 HKT as stated in paragraph 2 of Appendix C and are archived for at least 7 years.

   HKCA will exercise reasonable endeavours to serve a Revocation Notice to the Subscriber via the iAMSmartRO under Section 4.2.1.4.

b) A Subscriber must not use a certificate registered in his name after the occurrence of any of the following relevant events:

   (i) on becoming aware of any ground upon which HKCA could revoke it under the terms of this CPS (including those specified in Section 4.2.1.4); or

   (ii) the Subscriber has made a revocation request to HKCA via the iAMSmartRO in relation to such certificate under Section 4.2.2.1.

   HKCA and the iAMSmartRO shall be under no liability to the Subscriber or the Relying Parties in respect of any such transactions if the Subscriber uses the certificate in a transaction any time after the occurrence of any of the above relevant events.

c) Further, upon occurrence of any of the relevant events as specified in b) (i) to (ii) above, Subscribers must immediately notify the Relying Parties accordingly and that the Relying Parties shall not rely upon the certificate in respect of the transaction. HKCA and the iAMSmartRO shall be under no liability to the Subscribers and the Relying Parties regardless of whether or not the Subscriber has done so.

   HKCA and the iAMSmartRO shall be under no liability to the Subscriber and Relying Parties in respect of the transactions in the period between HKCA's decision to revoke a certificate (either in response to a request or acting on its own accord) and the appearance of the revocation status on the CRL or in the period between the decision to revoke a certificate and the updated return of the revocation status through OCSP response, and any transactions effected by any revoked iAM Smart-Cert any time thereafter.

d) The CRL and Authority Revocation List ("ARL") of HKCA is updated and published in accordance with the schedule and format specified in **Appendix C**.

4.2.4 Effective time of Revocation

Without prejudice to Sections 4.2.3b) to d) above, revocation terminates a certificate as at the actual time of the appearance of the revocation status on the CRL or the updated status of the revocation status through OCSP response. Regardless, HKCA and the iAMSmartRO will not be responsible for any usage of the certificate in breach of Section 4.2.3b) or other applicable provision notwithstanding the aforementioned effective time or any time thereafter. Relying Parties are reminded to check the Repository, the CRL and/or the relevant OCSP response before relying on a transaction effected through the use of an iAM Smart-Cert. However, where the iAMSmartRO has duly performed its duty as specified in Section 3.2.2, it should not be possible for an iAM Smart-Cert to be used in an unauthorised manner after it has been expired or revoked (where applicable).

4.3 Computer Security Audit Procedures

4.3.1 Types of Events Recorded

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

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

4.3.2 Frequency of Processing Log

Audit logs are processed and reviewed on a daily basis to provide audit trails of actions, transactions and processes of HKCA.

4.3.3 Retention Period for Audit Logs

Archived audit log files are retained for at least 7 years.

4.3.4 Protection of Audit Logs

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

4.3.5 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.

4.3.6 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.

4.3.7 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.

4.3.8 Vulnerability Assessments

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

4.4 Records Archival

4.4.1 Types of Records Archived

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

a) system equipment configuration files;
b) results of assessments and/or review for accreditation of the equipment (if conducted);
c) Certification Practice Statement and its modifications or updates;
d) contractual agreements to which HKCA is bound;
e) all certificates and CRLs as issued or published, and all OCSP responses;
f) periodic event logs;
g) other data necessary for verifying archive contents; and
h) documentation supporting certificate application, information on the approval and rejection of certificate services, and Subscriber Agreements.

4.4.2 Archive Retention Period

Key and certificate information is securely maintained for at least 7 years. Audit trail files are maintained in the CA systems as deemed appropriate by HKCA.

4.4.3 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.

4.4.4 Archive Backup Procedures

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

4.4.5 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.

4.5 Key Changeover

The HKCA's CA root certificate created by HKCA (See **Appendix E**) for the purpose of certifying

iAM Smart-Cert issued under this CPS have a lifespan of no more than 25 years starting from the creation of the HKCA's CA root certificate as specified in **Appendix E**. They will be renewed at least 3 months before their expiry. Upon renewal of a root key, the associated root certificate will be published in HKCA web site https://www.hkca.hk for public access. The original root keys will be kept for a minimum period as specified in Section 4.4.2 for verification of any signatures generated by the original root keys.

4.6 Disaster Recovery and Key Compromise Plans

4.6.1 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 CA services. This incorporates a tested independent disaster recovery site which is currently located at least 10km from the primary CA operational site within the territory of Hong Kong. The business continuity plans are reviewed and exercised annually.

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.

During the period of time following a disaster and before a secure environment is re-established, HKCA will not able to update the CRL nor return the OCSP responses. Subscribers may still continue to use iAM Smart-Cert but at their risks. HKCA will also not be able to issue certificate, to revoke certificate, or to make available the Repository to enable download of Public Keys and certificates.

4.6.2 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 any CA Private Key for the issuance of iAM Smart-Certs under this CPS has been compromised. The compromise of a CA Private Key will result in prompt revocation of the certificates issued under that Private Key and the issuance of new and replacement certificates.

4.6.3 Key Replacement

In the event of key compromise or disaster where any CA Private Key for the issuance of iAM Smart-Certs 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 CA Public Key is to be provided to the Subscribers, and how the Subscribers are to be re-issued with new certificates.

4.7 CA Termination

In the event that HKCA ceases to operate as a Recognized 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 CRLs for at least 7 years after the date of service termination.

According to the HKCA termination plan, HKCA will inform the Commissioner for Digital Policy its intention to terminate its services in relation to iAM Smart-Certs at least 90 days before the termination takes effect. HKCA will inform, by e-mail or letter mail or via iAM Smart System, all its Subscribers HKCA's intention to terminate its service as a Recognized CA at least 60 days before the termination takes effect. HKCA will advertise its intention to terminate its service as a Recognized CA in one English language daily newspaper (if available) and one Chinese language newspaper in circulation in Hong Kong for at least three consecutive days at least 60 days before the termination takes effect.

4.8 iAMSmartRO Termination

In the event that the iAMSmartRO, for whatever reason, ceases to act as the Registration Authority under this CPS, the iAM Smart-Cert issued through the iAMSmartRO will also be revoked at the same time. HKCA and iAMSmartRO shall not be responsible for any claim, legal proceeding, liability, loss (including any direct or indirect loss, any loss of revenue, profit, business, contract or anticipated saving), damage (including any direct, special, indirect or consequential damage of whatsoever nature) or any cost or expense, suffered or incurred by any person whomsoever due to the revocation.

5. PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY CONTROLS

5.1 Physical Security

5.1.1 Site Location and Construction

The HKCA CA operation is located in a site that affords commercially reasonably practical 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.

5.1.3 Power and Air Conditioning

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

5.1.4 Natural Disasters

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

5.1.5 Fire Prevention and Protection

The CA facility has a fire prevention plan and suppression system in place.

5.1.6 Media Storage

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

5.1.7 Off-site Backup

Adequate backups of the HKCA CA System data will be stored off-site and are afforded adequate protection against theft, destruction and media degradation (see also Section 4.6.1).

5.2 Procedural Controls

5.2.1 Trusted Role

Employees, contractors, and consultants of HKCA, of the iAMSmartRO and of the Contractor (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.

Procedures are established, documented and implemented for all trusted roles in relation to HKCA iAM Smart-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 the iAMSmartRO

All documents and data transmitted between HKCA, the iAMSmartRO and the Contractor are delivered in a control and secure manner using a protocol prescribed by HKCA and agreed by the iAMSmartRO as well as the Contractor from time to time.

5.2.3 Annual Assessment

An annual assessment is undertaken to confirm compliance with policy and procedural controls (see Section 2.4).

5.3 Personnel Controls

5.3.1 Background and Qualifications

HKCA, the iAMSmartRO and the Contractor follow personnel and management policies that provide reasonable assurance of the trustworthiness and competence of their personnel (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 iAMSmartRO and the Contractor to conduct investigations of personnel who serve in trusted roles (prior to their employment/engagement and periodically thereafter as necessary) to verify such personnel’s trustworthiness and competence in accordance with the requirements of this CPS. Personnel who fail an initial or periodic investigation are not permitted to serve or to continue to serve in a trusted role.

5.3.3 Training Requirements

HKCA personnel and those of the iAMSmartRO’s and the Contractor’s have received the initial training needed to perform their duties. HKCA, the iAMSmartRO and the Contractor also provide ongoing training as necessary to enable their respective personnel to remain current in required skills.

5.3.4 Documentation Supplied To Personnel

HKCA personnel and those of the iAMSmartRO’s and the Contractor’s receive comprehensive user manuals detailing the procedures for certificate creation, issuance, updating, renewal, and revocation, and other software functionality relative to their roles.

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 CA keys is implemented through physical security and secure key storage. The HKCA CA keys are generated, stored, used and destructed only within a tamper-proof hardware device, which is under multi-person access control.

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

CA root certificate Key Pairs for HKCA 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 CA root certificate Key Pairs for issuing iAM Smart-Certs that conform to this CPS. Applicant's Key Pairs for iAM Smart-Certs are generated by the iAMSmartRO in a HSM hosted in the iAM Smart System and an environment within the iAMSmartRO's premises.

6.1.2 Subscriber Public Key Delivery

In key generation of the Applicant/Subscriber's iAM Smart-Cert, the iAMSmartRO will generate the CSR containing the Public Key and transmits the CSR to HKCA through a system interface.

6.1.3 Public Key Delivery to Subscriber

The Public Key of each HKCA CA root certificate is available on-line at https://www.hkca.hk. HKCA utilizes protection to prevent alteration of those keys.

6.1.4 Key Sizes

The HKCA Sub CA Key Pair is 2048-bit RSA. Subscriber Key Pairs for iAM Smart-Certs are 2048-bit RSA.

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 of iAM Smart-Certs are used for Digital Signatures. Keys of HKCA CA root certificate (the key used to create or issue certificates that conform to this CPS) is used only for signing (a) certificates, (b) Certificate Revocation Lists. Besides, OCSP signer's certificate is used for signing the OCSP responses.

6.2 Private Key Protection

6.2.1 Standards for Cryptographic Module

HKCA CA root certificate Private Keys are created in a crypto module validated to at least FIPS 140-1 Level 4.

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 CA root certificate Private Keys. For backup of HKCA Private Keys, see Section 6.2.4 below.

6.2.4 Backup of HKCA Private Keys

Each HKCA CA root certificate Private Key is backed up by encrypting and storing it in devices which conform to FIPS 140-1 Level 4 security standard. Backup of the HKCA CA root certificate Private Key is performed in a manner that requires more than one person to complete. The backup Private Keys must be activated by more than one person. No other Private Keys are backed-up. All Private Keys will not be archived.

6.3 Other Aspects of Key Pair Management

HKCA CA root certificates and the associated keys will be used for no more than 25 years (see also Section 4.5). All HKCA key generation, key destruction, key storage, and certificate revocation list signing operations are performed in a hardware cryptographic module. Archival of HKCA CA root certificate Public Keys is performed as specified in Section 4.4.

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 HKCA CA System. Security procedures are in place to prevent and detect unauthorised access, modification, or compromise of the HKCA CA System. Such security controls are subject to compliance assessment as specified in Section 2.4.

6.5 Life Cycle Technical Security Controls

HKCA implements controls over the procedures for the procurement and development of software and hardware for HKCA CA System. Change control procedures are in place to control and monitor all revisions and enhancements to be made to the components of such system.

6.6 Network Security Controls

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

6.7 Cryptographic Module Engineering Controls

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

7. CERTIFICATE, CERTIFICATE REVOCATION LIST AND ONLINE CERTIFICATE STATUS PROTOCOL PROFILES

7.1 Certificate Profile

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

7.3 Online Certificate Status Protocol Profile

HKCA has delegated OCSP signing for the root CA “HKCA Root CA 1” to an OCSP responder by issuing an OCSP signer’s certificate containing the subject name “HKCA Root CA 1 OCSP Responder”. The OCSP signing for the Sub CA “HKCA d-Cert CA 1 - 26” is delegated to OCSP responders by issuing OCSP signer’s certificates containing the subject name “HKCA d-Cert CA 1 - 26 OCSP Responder”.

Details concerning the OCSP profile can be found in **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 CA web site at https://www.hkca.hk or in the HKCA Repository and are binding on all 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 CA web site at https://www.hkca.hk.

9. OTHER BUSINESS AND LEGAL MATTERS

This part describes the legal representations, warranties and limitations associated with iAM Smart-Certs.

9.1 Fees

9.1.1 Certificate issuance or renewal fees

iAM Smart-Cert is provided to the Subscriber for free.

9.1.2 Certificate access fees

HKCA reserves the right to establish and charge a reasonable fee for access to its database of certificates.

9.1.3 Revocation or status information access fees

HKCA does not charge fees for the revocation of a certificate or for a Relying Party to check the revocation status of a certificate through the use of CRLs or via OCSP.

9.1.4 HKCA's Liability for Received but Defective Certificates

Notwithstanding the limitation of HKCA's liability set out further below, if, after a Subscriber has received an iAM Smart-Cert, the Subscriber finds that, in respect of that iAM Smart-Cert, because of any error in the Private Key or Public Key of the certificate generated by iAMSmartRO, no transactions contemplated by the PKI can be completed properly or at all, and that Subscriber notifies the iAMSmartRO of this immediately to permit the certificate to be revoked and (if desired) re-issued, the iAM Smart-Cert will be re-issued to the Subscriber.

9.2 Financial responsibility

9.2.1 Insurance coverage

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

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

Without any intention to detract from its obligations under Section 46 of the Ordinance, specifically, HKCA keeps the following types of information confidential (collectively, "confidential information") and maintains reasonable controls to prevent the exposure of such records to non-trusted personnel.

a) all Private Keys of root-CA/sub-CA certificates owned and kept by HKCA for signing and issuance of certificates to Subscribers;
b) any business continuity, incident response, contingency, and disaster recovery plans;
c) any other security practices, measures, mechanisms, plans, or procedures used to protect the confidentiality, integrity or availability of information;
d) any information held by HKCA as private information in accordance with Section 9.4;
e) any transactional, audit log and archive record identified in Section 4.4.1, including certificate application records and documentation submitted in support of certificate applications whether successful or rejected; and
f) transaction records, audit records and external or internal audit trail records and any audit reports (with the exception of an auditor's letter confirming the effectiveness of the controls

set forth in this CPS).

9.3.2 Information not within the scope of confidential information

9.3.2.1 Subscriber application data which is published in an iAM Smart-Cert is considered public and not within the scope of confidential information. Subscribers acknowledge that revocation data of all certificates issued by the HKCA is published at the Repository and is public information.

9.3.2.2 HKCA does not possess the Private Keys of any of the iAM Smart-Certs as they are generated by iAMSmartRO and stored in the HSM hosted in the iAM Smart System and an environment within the iAMSmartRO's premises. Applicants and Subscribers are reminded that they should satisfy themselves concerning the security measures put in place by the iAMSmartRO for ensuring the confidentiality and security of the Private Keys before applying or renewing or accepting or using the iAM Smart-Certs.

9.4 Privacy of personal information

9.4.1 Privacy plan

HKCA has implemented a privacy policy, which is in compliance with this CPS. The HKCA privacy policy is published at https://www.hkca.hk/privacy-policy/.

9.4.2 Information treated as private

Personal information about an individual that is not publicly available in the contents of a certificate or CRL is considered private (collectively "private information").

9.4.3 Information not deemed private

Certificates, CRLs, and personal information appearing in the contents of a certificate or CRL are not considered private.

9.4.4 Notice and consent to use private information

HKCA may use private information with the subject's express written consent or as required by applicable law or court order or under other circumstances as set out in Section 46(2) of the Ordinance.

9.4.5 Disclosure pursuant to judicial or administrative process

HKCA shall not release any confidential information, unless as otherwise required under the circumstances specified in Sections 46(2)(a) to (d) of the Ordinance. Without intending to depart from the scope of the exceptions specified in Section 46(2) of the Ordinance, specifically, HKCA may disclose (a) confidential information to the iAMSmartRO, the Contractor or other contractor or consultant or advisor from time to time with a need to know in order to perform a function under or for the purpose of the Ordinance, or (b) confidential information in relation to a Subscriber or the Subscriber's certificate application, renewal and revocation to the iAMSmartRO.

9.5 Intellectual property rights

HKCA, the iAMSmartRO and the Contractor own all their respective intellectual property rights associated with their databases, systems, web sites and any other publication originating from HKCA including this CPS.

The trademarks "HKCA" and "HKCA d-Cert" are registered trademarks of HKCA. HKCA may have other trade and service marks that have not been registered, but that nonetheless are and shall remain the property of HKCA.

Certificates are the exclusive property of HKCA. HKCA gives permission to reproduce and distribute certificates on a non-exclusive, royalty-free basis, provided that they are reproduced and distributed in full. HKCA reserves the right to revoke the certificate at any time and at its sole discretion.

9.6 Representations and Warranties

9.6.1 HKCA Representations and Warranties

9.6.1.1 HKCA makes the following warranties and representations solely to Subscribers, and all Relying Parties that actually rely on such Certificate during the period when it is valid ("Certificate Warranties").

9.6.1.2 Subject to the limitations below, the Certificate Warranties specifically include warranties that:

(A) By issuing an iAM Smart-Cert, HKCA represents to any person who reasonably relies on the information contained in the iAM Smart-Cert or a Digital Signature verifiable by the Public Key listed in the iAM Smart-Cert, that HKCA has issued the Certificate in accordance with this CPS.

(B) By publishing an iAM Smart-Cert, HKCA represents to any person who reasonably relies on the information contained in the iAM Smart-Cert, that HKCA has issued the Certificate to the Subscriber identified in it.

9.6.1.3 HKCA does not warrant the accuracy, authenticity, completeness or fitness of any other information contained in Certificates or otherwise compiled, published, or disseminated by or on behalf of HKCA.

9.6.1.4 HKCA does not warrant the quality, functions or performance of any software or hardware device.

9.6.1.5 HKCA shall have no liability if it cannot execute the revocation of a Certificate for reasons outside its own control.

9.6.2 Subscriber representations and warranties

9.6.2.1 Each Subscriber must personally sign or confirm his acceptance of the Subscriber Agreement. As part of the Subscriber Agreement agreed to by a Subscriber, all of the following commitments and warranties are made and are deemed to have been made by that Subscriber for the express benefit of HKCA, the iAMSmartRO and all Relying Parties and are to be ensured to be true, complete and accurate by that Subscriber throughout the period of application, issuance and validity of the Certificate issued in his name:

(A) Accuracy of information: An obligation and warranty to provide accurate and complete information and other representations at all times to HKCA and the iAMSmartRO both in the application for an iAM Smart-Cert and as otherwise from time to time requested by HKCA (whether directly or via the iAMSmartRO) including without limitation those information and representations required in connection with the Issuance and Acceptance of the Certificate(s);

(B) Acceptance of Certificate: An obligation and warranty that the Subscriber will not use the Certificate until he has reviewed and verified the accuracy of the data in the Certificate;

(C) Use of Certificate: An obligation and warranty to use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement;

(D) Reporting and Revocation upon Compromise: An obligation and warranty to request that HKCA revoke the Certificate via the iAMSmartRO upon occurrence of any of the events specified in Section 4.2.1.4; and

(E) Termination of Use of Certificate: An obligation and warranty to immediately cease all use of the Certificate and his Private Key in accordance with Section 4.2.3(b).

9.6.2.2 Without limiting other Subscriber's obligations stated in this CPS, Subscribers are solely liable for any misrepresentations made by them in the Certificates to third parties that reasonably rely on the representations contained in the Certificates.

9.6.2.3 Upon Accepting a Certificate the Subscriber represents, warrants and covenants to HKCA, the iAMSmartRO and to Relying Parties that at the time of Acceptance and throughout the validity of the Certificate all of the following:

(A) transactions effectuated using the Private Key corresponding to the Public Key included in the Certificate are the acts of the Subscriber and that the Certificate has been accepted and is properly operational at that time throughout the validity of the Certificate.

(B) all representations made by the Subscriber to HKCA (whether directly or via the iAMSmartRO) and the iAMSmartRO are true, accurate and complete;

(C) all information contained in the Certificate is true, accurate and complete;

(D) the Certificate is used exclusively for authorised and legal purposes, consistent with this CPS, and that the Subscriber will use the Certificate for the usage specified in Appendix D;

(E) the Subscriber agrees with the terms and conditions of this CPS;

(F) the Subscriber abides by the laws applicable to his country or territory;

(G) the Subscriber has authorised the iAMSmartRO to keep the Subscriber's Private Key of the Certificate in custody and to access his Private Key whenever the Subscriber makes a Digital Signature;

(H) the Subscriber has prior to the use of Subscriber's Private Key of the Certificate submitted to strong authentication procedures stipulated by the iAMSmartRO for verifying his identity as a holder of iAM Smart; and

(I) each Digital Signature generated using the Subscriber's Private Key, which corresponds to the Public Key contained in the Subscriber's Certificate, is the Digital Signature of the Subscriber.

9.6.3 Relying party representations and warranties

A Relying Party accepts that in order to reasonably rely on an iAM Smart-Cert, the Relying Party must perform all of the following:

(A) make reasonable efforts to acquire sufficient knowledge on using digital certificates and PKI;

(B) study the limitations to the usage of digital certificates for the usage specified in Appendix D and be aware through this CPS of the limitations of liability of HKCA for reliance on the iAM Smart-Cert;

(C) verify that the Subscriber has a valid and unexpired iAM Smart-Cert by searching the Repository using the name of that person. Refrain from relying in an iAM Smart-Cert which is expired;

(D) verify the validity of the iAM Smart-Cert by referring to the CRL, or the relevant OCSP response whenever applicable. An iAM Smart-Cert which is revoked will have the corresponding status being shown as such in CRL or in relevant OCSP response. Refrain from relying on an iAM Smart-Cert which is revoked;

(E) take any other reasonable steps to minimize the risk of relying on a Digital Signature created by an invalid, revoked, expired or rejected iAM Smart-Cert which has been used in an unauthorised manner; and

(F) rely on an iAM Smart-Cert, only as may be reasonable under the circumstances given:

(a) any legal requirements for the identification of a party, the protection of the confidentiality or privacy of information, or the legal enforceability of the transaction in accordance with any laws that may apply;

(b) all facts listed in the Certificate, or of which the Relying Party has or should have notice, including this CPS;

(c) the economic value of the transaction;

(d) the potential losses or damage which might be caused by an erroneous identification or a loss of confidentiality or privacy of information in the application, transaction or communication;

(e) the applicability of the laws of a particular jurisdiction, including the jurisdiction specified in an agreement with the Subscriber or in this CPS;

(f) the Relying Party's previous course of dealing with the Subscriber, if any;

(g) usage of trade, including experience with computer-based methods of trade; and

(h) any other indicia of reliability or unreliability, or other facts of which the Relying Party knows or has notice, pertaining to the Subscriber and/or the application, communication or transaction.

9.7 Limitation of liability

9.7.1. It is the discretion of the Subscriber to determine within the mechanism provided by the iAMSmartRO (if any) the maximum value of the transaction which can be effected through the use of the iAM Smart-Cert. The iAM Smart-Cert itself poses no limit on the value of the transaction between the Subscriber and the Relying Party.

9.7.2 General Disclaimer: To the maximum extent permissible by law, HKCA and iAMSmartRO shall not be responsible for any claim, legal proceeding, liability, loss (including any direct or indirect loss, any loss of revenue, profit, business, contract or anticipated saving), damage (including any direct, special, indirect or consequential damage of whatsoever nature) or any cost or expense, suffered or incurred by any person whomsoever arising from or due to or in connection with or in relation to (a) the exercise of any function or power by HKCA as stated in this CPS; and (b) the use or reliance on any iAM Smart-Cert and (c) reliance or use of a false or forged Digital Signature of a Subscriber supported by an iAM Smart-Cert where HKCA has complied with the requirements of the Ordinance and the Code of Practice with respect to that certificate; and (d) unauthorised or dishonest or fraudulent use of an iAM Smart-Cert; (e) any information in the iAM Smart-Cert or in the Repository (other than the information required to be represented in Section 40 of the Ordinance) is untrue, inaccurate or incomplete.

9.7.3 Other than the representations specified in Sections 39 and 40 of the Ordinance, notwithstanding anything herein to the contrary, HKCA makes no other representation or warranty to any person (including any Subscriber, any Relying Parties, and any Contractor) including (a) any confirmation that any information on the Certificate or in the Repository (other than the information required to be confirmed in Section 40 of the Ordinance) is accurate, correct or complete; and (b) the validity or legality of any transactions transacted through the use of a Digital Signature through an iAM Smart-Cert.

9.7.4 Other than the representations specified in Sections 39 and 40 of the Ordinance, to the maximum extent permissible by law, HKCA disclaims any duty of care owed to any person (including any Subscriber, any Relying Party and any Contractor) whether under this CPS, under the Ordinance, or the Code of Practice or any Subscriber Agreement or otherwise at law. No action or omission of HKCA or its officers acting in the course of employment shall be considered as negligence or willful default actionable at the suit of any of them provided that there is no breach of the representations specified in Sections 39 and 40 of the Ordinance.

9.7.5 Apart from the representations set out in Sections 39 and 40 of the Ordinance and any other representation or warranty which cannot be excluded by law, HKCA disclaims all representations, warranties and obligations of any type, including any warranty of fitness for a particular purpose, and any warranty of the accuracy of unverified information provided.

9.7.6 **In case of any non-compliance with or breach of the CPS or the Subscriber Agreement or Section 39 or 40 of the Ordinance, HKCA's liability to the Subscriber for legally recognized and provable claims for losses or damage suffered by the Subscriber as a result of any one or more of the above-mentioned non-compliance or breach shall not exceed HK$200,000 (in aggregate, if more than one non-compliance or breach) in respect of one iAM Smart-Cert, or HK$0 in respect of one iAM Smart-Cert (Minor) issued to a person under 18.**

9.7.7 **In case of any non-compliance with or breach of the CPS or any representation specified in Section 39 or 40 of the Ordinance, HKCA's liability to a Relying Party for legally recognized and provable claims for losses or damage suffered by the Relying Party as a result of any one or more of the above-mentioned non-compliance or breach shall not exceed HK$200,000 (in aggregate, if more than one non-compliance or breach) in respect of one iAM Smart-Cert, or HK$0 in respect of one iAM Smart-Cert (Minor) issued to a person under 18.**

9.7.8 The Contractor is a contractor appointed by HKCA pursuant to a separate contract between HKCA and the Contractor and the appointment is on the terms of that separate contract alone. Nothing in this CPS shall give any additional right to the Contractor, or impose additional obligation on HKCA to the Contractor. As for the representations in Sections 39 and 40 of the Ordinance, it is the duty of the Contractor to ensure that they are complied with to the extent that the Contractor performs any function for HKCA as stated therein. The Contractor is not a person who reasonably relies on the information contained in the certificate as mentioned in Section 40 of the Ordinance.

9.7.9 All Applicants, Subscribers, the Contractor, Relying Parties, and other persons, entities, and organisations acknowledge that but for the disclaimers of representations, warranties, and conditions and the limitations of liability set out in Sections 9.7 and 9.8, HKCA would not issue Certificates to Subscribers, that neither would HKCA provide services in respect to Certificates, and that these provisions are necessary to provide for a reasonable allocation of risk.

9.7.10 Each of provisions in Sections 9.7 and 9.8 shall be construed independently and without prejudice to any other provision of this CPS and, except where expressly stated otherwise, shall not be limited by reference to or inference from any other provision of this CPS.

9.8 Disclaimer of liabilities and limitation on the types of recoverable losses

9.8.1 Without prejudice to the generality of the disclaimers set out in Section 9.7, in no event and under no circumstances (except for fraud or willful misconduct) shall HKCA or iAMSmartRO be liable for any or all of the following and the results thereof:

9.8.1.1 any indirect, incidental or consequential losses or damage (even if HKCA or iAMSmartRO has been advised of the likelihood of such loss or damage in advance);

9.8.1.2 (whether considered as direct or indirect loss) any loss of profits or loss or injury to

reputation or goodwill or loss of opportunity or chance, loss of project;

9.8.1.3 any death or personal injury (save and except for any negligence of the HKCA or iAMSmartRO and "negligence" as defined in the Control of Exemption Clauses Ordinance (Cap. 71));

9.8.1.4 any loss of data;

9.8.1.5 any other indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, performance or non-performance of Certificates or Digital Signatures;

9.8.1.6 any claim, proceeding, loss or damage (direct or indirect or incidental or consequential special) except for those due to reliance on, the representations set out in Sections 39 and 40 of the Ordinance;

9.8.1.7 any claim or liability incurred arising from reliance on the Certificate or any information in the Certificate or Repository where any irregularity is due to fraud or willful misconduct of the Applicant or Subscriber or any other person;

9.8.1.8 any liability that arises from the usage of a Certificate that has not been used in conformance with this CPS;

9.8.1.9 any liability that arises from the usage of a Certificate that is not valid (which has expired or revoked);

9.8.1.10 any liability that arises from the usage of a Certificate that exceeds any applicable limitations in usage;

9.8.1.11 any liability that arises from the security, usability, integrity of products, including hardware and software an Applicant / Subscriber uses; and

9.8.1.12 any liability that arises from the compromise of the Private Key in relation to any Certificate.

9.8.2 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 or services to Relying Parties and likewise gives no warranty to Relying Parties 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 or services to Relying Parties.

9.8.3 Time Limit for Making Claims

Without prejudice to the disclaimers and limitations set out in Sections 9.7 and 9.8 and elsewhere in this CPS, any Subscriber or Relying Party or any other person who wishes to make any legal claim upon HKCA arising out of or in any way connected with the issuance, revocation or publication of an iAM Smart-Cert must do so within one year of the date upon which it 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, it could have become aware of such facts. For the avoidance of doubt, ignorance of the legal significance of those facts is immaterial. After the expiration of this one-year time limit the claim shall be waived and absolutely barred.

9.8.4iAMSmartRO, the Contractor, and their Personnel

Neither the Government, nor any officer or employee or other agent of the Government (apart from the HKCA), is to be a party to the Subscriber Agreement. The Subscriber and Relying Parties must acknowledge that neither the Government nor any of its officers, employees or agents (including those officers, employees and agents of iAMSmartRO) voluntarily accepts or will accept any personal responsibility or duty of care to the Subscriber or Relying Parties in connection with any action or omission done in good faith by any of them in any way connected either with the performance of HKCA of a Subscriber Agreement or any certificate issued by HKCA as a Recognized CA. Each and every Subscriber and Relying Party undertakes to the Government and its officers and employees and agents (including those officers, employees and agents of iAMSmartRO) not to sue or seek any form of recovery or redress by other legal means whatsoever from any of them 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 Recognized CA, and acknowledges that HKCA has a sufficient legal and financial interest to protect these organisations and individuals from such actions.

9.8.5 Liability for Fraud

Any liability for fraud of HKCA is not within the scope of any limitation or exclusionary provision of this CPS, any Subscriber Agreement or Certificate issued by HKCA and is not limited or excluded by any such provision.

9.8.6 Certificate Notices, Limitations and Reliance Limit

Without prejudice to the binding effect of the remaining provisions of this CPS, iAM Smart-Certs issued by HKCA shall be deemed to have contained all provisions set out in Sections 9.6 to 9.15 of this CPS.

9.9 Indemnities

By accepting or using or relying on a Certificate, each Subscriber and each Relying Party agrees to indemnify and hold HKCA, as well as the Government and the officers, employees, agents, and contractors of the Government (including those of iAMSmartRO) harmless from all and any liabilities, all and any losses, damage and indebtedness, and all and any claims, legal proceedings, and costs, charges and expenses of any kind, including legal fees on a full indemnity basis, that HKCA, and/or the above mentioned parties may incur, that are caused by the use or publication of a Certificate, and that arises from that party's: (i) misrepresentation or omission of material fact in order to obtain or use a Certificate (whether such misrepresentation or omission was intentional or due to negligence or recklessness); (ii) violation of the Subscriber Agreement, this CPS, or any applicable law; (iii) compromise or unauthorised use of a Certificate or Private Key caused by the negligence of that party and not by HKCA; or (iv) misuse of the Certificate or Private Key.

9.10 Term and termination

9.10.1 Term

This CPS and any amendments hereto shall become effective upon publication by HKCA in the HKCA CA website at https://www.hkca.hk or in the Repository, and shall remain in effect perpetually until terminated in accordance with this Section 9.10.

9.10.2 Termination

This CPS as amended from time to time shall remain in force until it is replaced by a new version

or is otherwise terminated in accordance with this Section 9.10.

9.10.3 Effect of termination and survival

The conditions and effect resulting from the termination of this CPS will be communicated via the HKCA Repository (https://www.hkca.hk) upon termination. That communication will outline the provisions that may survive termination of this CPS and remain in force. The responsibilities for protecting business confidential and private personal information shall survive termination, and the terms and conditions for all existing Certificates shall remain valid for the remainder of the validity periods of such Certificates.

It is hereby declared that no person's consent is required for the HKCA's termination of this CPS.

9.11 Individual notices and communications with participants

HKCA accepts notices related to this CPS by means in electronic form or in paper form addressed to the locations specified in Section 1.3 of this CPS. Upon receipt of a valid acknowledgment of receipt from HKCA, the sender of the notice shall deem their communication effective.

9.12 Amendments

9.12.1 All changes to this CPS will be published by HKCA who has the power to determine such changes. **It is hereby declared that no person's consent is required for the HKCA's changes to this CPS.** The CPS changes will be effective upon publication by HKCA in the HKCA CA web site at https://www.hkca.hk or in the HKCA Repository and are binding on all Applicants, Subscribers, the iAMSmartRO, Relying Parties, the Contractor and other parties who may be treated as third parties under the Subscriber Agreement without any prior reference to, or consent from, any of them. 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 on the HKCA CA web site at https://www.hkca.hk. **For those Subscribers who do not agree with any changes to the CPS as aforementioned, they have a period of one month following from such changes coming into effect to issue a notice to HKCA to cease using the iAM Smart-Cert under Section 4.2.2.1 and revoke the iAM Smart-Cert via the iAMSmartRO. The absence of any such notice on the part of a Subscriber within the aforesaid one-month period shall be taken as agreement of the Subscriber with such changes.**

9.12.2 The Subscriber Agreement cannot be varied, amended or changed unilaterally by any party except by HKCA to comply with a variation or change in this CPS. Subject to the foregoing, all other changes must be agreed by the parties to the Subscriber Agreement. No consent from any third parties shall be required for any amendment as mentioned above (whether by HKCA unilaterally or by agreement between the Subscriber and HKCA).

9.12.3 No consent from any third parties shall be required for any termination of the Subscriber Agreement or termination or revocation of any iAM Smart-Cert by a party in accordance with the terms of the CPS (whether by HKCA or by a Subscriber unilaterally or by agreement between HKCA and the Subscriber).

9.12.4 Reasonable steps have been taken to make these third parties to be aware of this Section 9.12 through publication of the CPS.

9.13 Dispute Resolution

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

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

9.14 Governing law

This CPS is governed by and construed in accordance with the laws of Hong Kong. This choice of law is made to ensure uniform interpretation of this CPS, regardless of the place of residence or place of use of HKCA digital certificates.

Each of the parties hereto agrees to submit to the exclusive jurisdiction of the courts of Hong Kong for resolving any disputes which may arise out of or in connection with this CPS or the Subscriber Agreement.

9.15 Entire agreement

9.15.1 This CPS shall be interpreted consistently within the boundaries of business customs, commercial reasonableness under the circumstances, and intended usage of the product or service described herein. In interpreting this CPS the parties shall also take into account the scope and application of the services and products of HKCA as well as the principle of good faith as it is applied in commercial transactions. Notwithstanding the foregoing, the certification practice statements issued by HKCA for other types of certificates shall not be referred to in the interpretation of the provisions set out in this CPS.

9.15.2 The headings, subheadings, and other captions in this CPS are intended for convenience and reference only and shall not be used in interpreting, construing, or enforcing any of the provisions of this CPS.

9.15.3 Appendices and definitions to this CPS are for all purposes an integral and binding part of the CPS.

9.15.4 If/when this CPS (as from time to time amended) conflicts with other rules, guidelines, or contracts, this CPS shall prevail (save to the extent the provisions of this CPS are prohibited by the Ordinance) and bind the Subscriber and other parties. If there is any conflict between the sections of this CPS and any other document that relate to HKCA, then the sections benefiting HKCA and preserving HKCA's best interests, at HKCA's sole determination, shall prevail and bind the applicable parties.

9.16 Assignment

Parties to this CPS may not assign any of their rights or obligations under this CPS or applicable agreements without the written consent of HKCA.

9.17 Severability

9.17.1 If any provision of this CPS or the application thereof, is for any reason and to any extent found to be invalid or unenforceable, the remainder of this CPS shall remain in full force and effect and shall be interpreted in such manner as to implement the original intention of the parties to the fullest extent possible.

9.17.2 Each and every provision of this CPS that provides for a limitation or disclaimer of liability or exclusion of damages is intended to be severable and independent of any other provision and is to be enforced as such.

9.18 Enforcement (attorneys' fees and waiver of rights)

HKCA reserves the right to seek indemnification and legal fees from any party related to that party's conduct described in Section 9.9. Except where an express time frame is set forth in this CPS, no delay or omission by any party to exercise any right, remedy or power it has under this CPS shall impair or be construed as a waiver of such right, remedy or power. A waiver by any party of any breach or covenant in this CPS shall not be construed to be a waiver of any other or succeeding breach or covenant. Bilateral agreements between HKCA and the parties to this CPS may contain additional provisions governing enforcement.

9.19 Force Majeure

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

9.20 Other provisions

9.20.1 This CPS shall be binding upon the successors, executors, heirs, representatives, administrators, and assigns, whether express, implied, or apparent, of the parties that this CPS applies to.

9.20.2 Retention of Title

The title, copyright, and intellectual property rights to the certificate are and will remain vested in HKCA.

9.20.3 Fiduciary Relationships

None of HKCA, the iAMSmartRO, or the Contractor is an agent, fiduciary, trustee or other representative of the Subscribers or Relying Parties at any time. The Subscribers and Relying Parties have no authority to bind HKCA, the iAMSmartRO or the Contractor, by contract or otherwise, to any obligation as an agent, fiduciary, trustee or other representative.

9.20.4 Interpretation

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

Appendix A - Glossary

Definitions

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

"Accept" (upper or lower case), in relation to a certificate

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

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

"Applicant" means a natural person who has applied for an iAM Smart-Cert. Once the iAM Smart-Cert is issued, the Applicant is referred to as the Subscriber.

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

"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.

"Certificate" (upper or lower case) **or "iAM Smart-Cert"** means a Record which:-

(a) is issued by HKCA for the purpose of supporting a Digital Signature which purports to confirm the name of the person stated therein is the person authorised to use the Private Key corresponding to the Public Key contained in the certificate.
(b) identifies the HKCA as 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 HKCA as the Certification Authority issuing it.

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

"Certification Practice Statement" or "CPS" means this document including all Appendices thereto.

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

"**Certificate Signing Request**" or "**CSR**" means a message generated by the iAMSmartRO, upon receiving the Applicant's iAM Smart-Cert application, and sent to HKCA via the iAM Smart System in order to apply for a Certificate.

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

"Contract" means the outsourcing contract which HKCA from time to time enters into with a contractor for performing all or any of the functions of the HKCA as stipulated in this CPS on behalf of HKCA under the overall supervision and management of HKCA.

"Contractor" means the contractor to the Contract as from time to time entered into by HKCA; and all sub-contractors of such contractor;

"Correspond", in relation to Private or Public Keys, means to belong to the same Key Pair.

"CRL" means Certificate Revocation List.

"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.

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

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

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

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

"HKID Card" means an identity card issued under the Registration of Persons Ordinance (Cap. 177).

"HKCA" means Hong Kong Certification Authority as a Recognised Certification Authority in the Ordinance.

"HKCA CA System" means the computer hardware, software and procedures used by HKCA to perform the CA functions.

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

"holder of iAM Smart" means a person who has obtained iAM Smart in accordance with Section 3.1.1 and the iAM Smart remains valid in the iAM Smart System.

"HK$" or Hong Kong Dollars" means the lawful currency of Hong Kong.

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

"iAM Smart" means the electronic identity provided by the Hong Kong Government for Hong Kong residents to conduct electronic transactions. In this CPS, **iAM Smart** refers to the version

of iAM Smart obtained in accordance with Section 3.1.1.

"iAM Smart Registration Point" means a registration point provided by the iAMSmartRO at designated premises with designated devices for the Hong Kong residents to appear in-person to register for iAM Smart version that is eligible for applying the iAM Smart-Cert.

"iAM Smart System" means the system developed and managed by the Government (through contractor(s) appointed by the iAMSmartRO) which offers iAM Smart functions including registration, usage and account maintenance to Hong Kong residents.

"iAMSmartRO" means the iAM Smart Registration Office referred to in Section 1.2.2.

"**Immigration Department**" means the Immigration Department of the Government of Hong Kong.

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

"Information System" means a system which -

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

"Issue" (upper or lower case) in relation to a certificate, means to:

(a) create the certificate, and then notify directly or indirectly via the iAMSmartRO 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 directly or indirectly via the iAMSmartRO 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.

"Near Field Communication" or **"NFC"** means a wireless technology that enables a variety of contactless and proximity-based applications, such as payments, information retrieval, mobile marketing and device pairing.

"Online Certificate Status Protocol" or **"OCSP"** means an online certificate checking protocol that enables the status of a certificate to be checked.

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

"organisation" means any entity other than an individual;

"**PKI**" means Public Key infrastructure

"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.

"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" or **"Recognized CA"** means a Certification Authority recognized under Section 21 and 27, or the Certification Authority referred to in Section 34, of Electronic Transactions Ordinance.

"Record" (upper or lower case) 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" or **"RA"** means an entity that acts on behalf of HKCA in carrying out registration function to authenticate Applicants prior to the issuance of iAM Smart-Cert.

"Reliance Limit" means the monetary limit specified for reliance on an iAM Smart-Cert in the amount as specified in Section 9.7.

"Relying Party" means a person who may reasonably relies on the information contained in an iAM Smart-Cert by complying with the warranties and representations specified in Section 9.6.3.

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

"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.

"Smartphone equipped with NFC function", in respect of iAM Smart usage, means a facility with the approval of the Government granted under Section 12(1B) of the Registration of Persons Regulations (Cap. 177A) to gain access to the data in the chip of the HKID Card of a person to whom the HKID Card relates during specified circumstances.

"**SRN**" means a Subscriber Reference Number generated by the HKCA system.

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

"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) has authorised the iAMSmartRO to hold the Private Key which corresponds to a Public Key listed in that certificate.

Note:- "holds", in connection to a Private Key as referred in this CPS, means to keep in one's custody such that only the person named or identified in a certificate can use that Private Key.

"Subscriber Agreement", in respect of iAM Smart-Cert, means an agreement between HKCA and the Subscriber of such certificate, which comprises the Subscriber Terms and Conditions of iAM Smart-Cert and 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.

2. Interpretation Principles

2.1 In this CPS, unless the context otherwise requires, the following rules of interpretation shall apply:

(a) references to statutes or statutory provisions shall be construed as references to those statutes or statutory provisions as replaced, amended, modified or re-enacted from time to time; and shall include all subordinate legislation made under those statutes;

(b) words importing the singular shall include the plural and vice versa; words importing a gender shall include all other genders; references to any person shall include references to any individual, firm, body corporate or unincorporate (wherever established or incorporated);

(c) clauses headings are inserted for convenience of reference only and shall not affect the construction of this CPS;

(d) references to a document shall:

(i) include all schedules, appendices and annexures attached to such document; and

(ii) mean the same as from time to time validly amended or supplemented;

(e) references to "Subscriber" or "Applicant" or "Relying Party" or "Contractor" shall include its permitted assigns, successors-in-title, or any persons deriving title under it;

(f) references to "HKCA" or "iAMSmartRO" shall include its assigns, successors-in-title, and persons deriving title under it, regardless of whether or not any of these persons are mentioned separately in the relevant provisions;

(g) references to Sections, Appendices and Annexes shall, unless otherwise specified, mean the sections of, and appendices and annexes to, this CPS;

(h) references to "laws", "regulations" or "law" shall include any constitutional provisions, treaties, conventions, ordinances, subsidiary legislation, orders, rules and regulations having the force of law and rules of civil and common law and equity;

(i) a time of day shall be construed as a reference to Hong Kong time;

(j) references to a day shall be construed as a calendar day; references to a working day shall be construed as any calendar day other than Saturday, all general holidays by virtue of the General Holiday Ordinance (Cap.149), and all days on which a black rainstorm warning signal is issued or tropical cyclone signal No. 8 or above is hoisted; references to a month or a monthly period mean a calendar month;

(k) words importing the whole shall be treated as including a reference to any part of the whole;

(l) the expressions "include" and "including" shall mean including without limitation basis regardless of whether it is expressly so provided;

(m) words and expressions extend to their grammatical variations and cognate expressions where those words and expressions are defined in this CPS or by reference to any other definition;

(n) references to “writing” include typewriting, printing, lithography, photography, facsimile and the printed out version of a communication by electronic mail and other modes of representing and reproducing words in a legible form; and

(o) references to “Cap” or “Chapter” followed by a number mean a chapter of the Laws of Hong Kong.

2.2 Nothing in this CPS shall be taken to restrict, derogate from or otherwise interfere with any power or duty, or the exercise or performance of any power or duty conferred or imposed by or under any law upon HKCA.

Appendix B - HKCA iAM Smart-Cert Format

This appendix provides the formats of iAM Smart-Cert issued by the Sub CA "HKCA d-Cert CA 1 - 26" under this CPS.

A. iAM Smart-Cert Certificate Format

Field Name		Field Content	
		HKCA iAM Smart-Cert certificates	**HKCA iAM Smart-Cert (Minor) certificates issued to persons aged under 18**
Standard fields			
Version		X.509 v3	
Serial number		[20-byte hexadecimal number randomly generated by HKCA system]	
Signature algorithm ID		sha256RSA	
Issuer name		cn=HKCA d-Cert CA 1 - 26 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) ou=[SRN] (Note 2) o=HKCA iAM Smart-Cert c=HK	cn=[HKID name] (Note 1) ou=[SRN] (Note 2) o=HKCA iAM Smart-Cert (Minor) (Note 3) 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 4)			
Authority Information Access	**Certification Authority Issuer**	[URL of the Issuer's public certificate]	
	OCSP	[URL of the OCSP Responder](Note 9)	
Authority key identifier		[Subject Key Identifier of the issuer's certificate]	
Key usage		Digital Signature, Non-repudiation **(This field will be set Critical.)**	
Certificate policies		Policy Identifier =[OID](Note 5) Policy Qualifier Id = CPS Qualifier : [URL of CPS] Policy Identifier = 1.3.6.1.4.1.64092.1.4(Note 6) Policy Qualifier Id = CPS Qualifier = [URL of CPS]	
Subject alternative name	**DNS**	encrypted(HKID) (Note 7)	
Issuer alternative name		Not used	
Basic constraints	**Subject type**	End Entity	
	Path length constraint	None	
Extended key		SSL Client	

usage		
CRL distribution points		Distribution Point Name = [URL of CRL Distribution Point] (Note 8)

Note

1. Applicant name format: Surname (in capital) + Given name (e.g. CHAN Tai Man David).
2. SRN: 10-digit Subscriber Reference Number
3. "iAM Smart-Cert (Minor)" indicates that the Applicant is under 18 at the time the iAM Smart-Cert is issued (see Section 3.1.3 of this CPS).
4. All standard extensions are set as "non-critical" unless otherwise specified.
5. The OID of this CPS is included in this field. Please refer to Section 1.1 of this CPS for the OID of this CPS.
6. The OID for supporting Adobe PDF signing is included in this field.
7. 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:

   $$cert\_hkid\_hash = SHA\text{-}256\ (\ RSA_{privatekey,\ sha\text{-}256}(\ hkid\_number\ )\ )$$

   where the SHA-256 is a hash function and RSA is the signing function
8. URL of CRL Distribution Point of is http://crl.hkca.hk/crl/HKCAdCertCA1-26CRL_<xxxxx>.crl which are partitioned CRLs issued by the Sub CA "HKCA d-Cert CA 1 - 26", 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 revoked, its information will be published in the partitioned CRL at the URL specified in this CRL Distribution Point field.
9. URL of OCSP responder is: http://ocsp.hkca.hk

Appendix C - HKCA Certificate Revocation Lists (CRLs) and Authority Revocation List (ARL) and Online Certificate Status Protocol (OCSP) Response Format

The Appendix C of this CPS provides the arrangement of updating and publishing as well as the format of the Certificate Revocation Lists (CRLs) that are issued by the Sub CA "HKCA d-Cert CA 1 - 26", and the Authority Revocation List (ARL) that is issued by the root CA "HKCA Root CA 1".

Moreover, HKCA has delegated OCSP signing for the root CA "HKCA Root CA 1" to an OCSP responder by issuing an OCSP signer's certificate containing the subject name "HKCA Root CA 1 OCSP Responder". The OCSP signing for the Sub CA "HKCA d-Cert CA 1 - 26" is delegated to an OCSP responder by issuing an OCSP signer's certificate containing the subject name "HKCA d-Cert CA 1 - 26 OCSP Responder". Furthermore, a unique OID "**1.3.6.1.4.1.64092.1.6**" is assigned to the OCSP responders and specified in the field "Certificate Policies" of the OCSP signer's certificate. In the last section of this Appendix C, the format of OCSP response is also provided.

HKCA updates and publishes the following Certificate Revocation Lists (CRLs) containing information of iAM Smart-Certs revoked under this CPS 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)) upon the iAM Smart-Cert is revoked:-

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

- iAM Smart-Cert issued by Sub CA "HKCA d-Cert CA 1 - 26":
  http://crl.hkca.hk/crl/HKCAdCertCA1-26CRL_<xxxxx>.crl
  where <xxxxx> is a string of five alphanumeric characters.

b) **Full CRL** that contains information of all revoked certificates that are issued by the Sub CA "HKCA d-Cert CA 1 - 26". The Full CRL is available at :-

- iAM Smart-Cert issued by Sub CA "HKCA d-Cert CA 1 - 26":
  http://crl.hkca.hk/crl/HKCAdCertCA1-26CRL.crl or
  ldap://ldap.hkca.hk (port 389, cn=HKCA d-Cert CA 1 - 26 CRL, o=Hong Kong Internet Registration Corporation Limited, c=HK)

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

Under normal circumstances, HKCA 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 web site on ad hoc basis without prior notice.

Format of Partitioned and Full CRL issued by the Sub CA "HKCA d-Cert CA 1 - 26" 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 - 26, 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.

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

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

- 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)

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.)**	

Format of OCSP response under this CPS :

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

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

		Next update	[GeneralizedTime]	Date and Time for new updates to be made available (GMT+0).
Signature algorithm ID			sha256RSA	Algorithm that was used to sign this response.
Signature			[Signature data]	Signature of this response
Certificate			[Responder signing certificate data]	Responder's signing certificate

Note

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

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

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

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

Appendix D - Summary of HKCA iAM Smart-Cert Features

Features	iAM Smart-Cert Certificate
Subscriber	HK residents who are holders of iAM Smart (refer to Section 3.1.1)
Authorised user of the Certificate	Same as Subscriber
Reliance Limit	▪ HK$200,000 in respect of one iAM Smart-Cert, or ▪ HK$0 in respect of one iAM Smart-Cert (Minor) issued to a person under 18. (refer to Sections 9.7.6 and 9.7.7)
Recognized Certificate	Yes
Key pair size	2048-bit RSA
Key pair generation	Key generation by iAMSmartRO
Identity verification at the time of application for the iAM Smart-Cert	as mentioned in Section 4.1.1
Usage of certificate	Non-repudiable Digital Signature
Subscriber's information included in the certificate	▪ Name of the Subscriber; ▪ HKID of the Subscriber encrypted as a hash value; and ▪ Subscriber Reference Number (SRN) generated by the HKCA system.
Subscription fees and Administration fees	Free
Certificate validity	One year

Appendix E- 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 - 26	[TBC]	This Sub CA commences to issue iAM Smart-Cert to applicants with effect from [TBC].