



Independent practitioner's assurance report

To the management of Hong Kong Internet Registration Corporation Limited ("HKIRC"):

Scope

We have been engaged to perform a reasonable assurance engagement on [the assertions by the management of HKIRC](#) and [Certizen Limited \("Certizen"\)](#) (the "assertions"), an independent subservice organization that provides operation and maintenance services to HKIRC, that in generating and protecting its HKCA Root CA 3, HKCA Root CA 4, HKCA Root CA 5 and HKCA Root CA 6 (collectively, "HKIRC Root CAs") on 15 September 2026, in the Hong Kong Special Administrative Region of China, with the following identifying information:

Root Name	Subject Key Identifier	Certificate Serial Number
HKCA Root CA 3	CC1672E379FB74F2AF5F176F8B44 A1DC49EAA66C	31BE0C66A1EAEAACC4F3EFC4 E5E598FE7CD3BB6B
HKCA Root CA 4	A7106D800B50D411C40AA94DDC35 0E463F2CE992	1FC8DE343A5BFAC64A2677A3E F96F1515F3B57EF
HKCA Root CA 5	5E12B37043EA17418D6456B9A0FC 040044CD1D24	2103625EA3498B77C63E5F710E 99D4B61184D17E
HKCA Root CA 6	BA991D2FC1464179609FBFB38724 1CAB71E9D15A	6ACBBF661D6E5D4D86F03D5DC D975FFA211E36B3

HKIRC with Certizen as its subservice organization has:

- followed the CA key generation and protection requirements in its certification practice statements as enumerated in [Attachment A](#);
- included appropriate, detailed procedures and controls in the HKCA S/MIME and Backup Root Key Generation Plan v3, 15 September 2026;
- maintained effective controls to provide reasonable assurance that the HKIRC Root CA keys were generated and protected in conformity with the procedures described in its CPS and its Root Key

Generation Script;

- performed, during the root key generation process, all procedures required by the Root Key Generation Script;
- generated the CA keys in a physically secured environment as described in its CPS;
- generated the CA keys using personnel in trusted roles under multiple person control and split knowledge;
- generated the CA keys within cryptographic modules meeting the applicable technical and business requirements as disclosed in its CPS,

in accordance with CA Key Generation Criterion 4.1 of the [WebTrust Principles and Criteria for Certification Authorities v2.2.3](#).

HKIRC uses Certizen (subservice organization) to provide operation and maintenance services. The controls at Certizen, are necessary, in combination with controls at HKIRC, for HKIRC to achieve the applicable WebTrust Criteria as set out in the assertions.

Certification Authority's Responsibilities

HKIRC's management is responsible for its management's assertion, including the fairness of its presentation, and for generating and protecting its CA keys in accordance with CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.2.3.

Subservice Organization's Responsibilities

Certizen has provided an accompanying assertion titled "Certizen Limited ("Certizen") Management's Assertion" (Certizen assertion) about the services provided to HKIRC. Certizen Management is responsible for its assertion and providing services in accordance with the described practices of HKIRC and designing, implementing, operating, and documenting controls in accordance with HKIRC's requirements, which enable HKIRC to achieve the applicable WebTrust Criteria as set out in the assertions.

Our Independence and Quality Management

We have complied with the independence and other ethical requirements of the Code of Ethics for Professional Accountants issued by the Hong Kong Institute of Certified Public Accountants (the “HKICPA”), which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

Our firm applies Hong Kong Standard on Quality Management 1 as issued by the HKICPA, which requires the firm to design, implement and operate a system of quality management including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Practitioner’s Responsibilities

It is our responsibility to express an opinion on the assertions by the management of HKIRC and Certizen based on our work performed.

We conducted our work in accordance with Hong Kong Standard on Assurance Engagements 3000 (Revised) “Assurance Engagements Other Than Audits or Reviews of Historical Financial Information” issued by the HKICPA. This standard requires that we plan and perform our work to form the opinion.

A reasonable assurance engagement involves performing procedures to obtain sufficient appropriate evidence whether the assertions are fairly stated, in all material respects, in accordance with CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.2.3. The extent of procedures selected depends on the practitioner’s judgment and our assessment of the engagement risk. Within the scope of our work we performed amongst others the following procedures: (1) obtaining an understanding of HKIRC’s documented plan of procedures to be performed for the generation of the certification authority key pairs for the HKIRC Root CAs; (2) reviewing the detailed CA key generation script for conformance with industry standard practices; (3) testing and evaluating, during the CA key generation process, the effectiveness of controls over the integrity, confidentiality, and availability of all private keys, including back-up copies, and access keys (including physical keys, tokens, and passwords), used in the establishment of the service (4) physical observation of all procedures performed during the root key generation process to ensure that the procedures actually performed on 15 September 2026 were in accordance with the Root Key Generation Script for the HKIRC Root CAs; and (5) performing such other procedures as we considered necessary in the circumstances.

The relative effectiveness and significance of specific controls and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other

factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Inherent Limitation

Because of the nature and inherent limitations of controls, HKIRC and Certizen's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorised access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any opinion based on our findings to future periods is subject to the risk that changes may alter the validity of such opinion.

Opinion

In our opinion, as of 15 September 2026, the assertions by the management of HKIRC and Certizen, as referred to above, are fairly stated, in all material respects, in accordance with CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.2.3.

This report does not include any representation as to the quality of HKIRC's services beyond those covered by CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.2.3, nor the suitability of any of HKIRC's services for any customer's intended purpose.



PricewaterhouseCoopers

Certified Public Accountants

Hong Kong, 16 October 2026

Attachment A

The list of Certification Practice Statements in scope is as follows:

No.	Document Names
1	<u>CPS for d-Cert (Personal) (Organisational) (Encipherment)</u>
2	<u>CPS for d-Cert (Server)</u>
3	<u>CPS for SMIME d-Cert (Personal) (Organisational) (Encipherment)</u>
4	<u>CPS for SMIME g-Cert</u>

Hong Kong Internet Registration Corporation Limited Management's Assertion

Hong Kong Internet Registration Corporation Limited ("HKIRC") has deployed a public key infrastructure. As part of this deployment, it was necessary to create a hierarchy consistent of self-signed Root CAs known as HKCA Root CA 3, HKCA Root CA 4, HKCA Root CA 5 and HKCA Root CA 6 (collectively, "HKIRC Root CAs"). These CAs will serve as Root CAs for client certificate services. In order to allow the CAs to be installed in a final production configuration, a Root Key Generation Ceremony was conducted, the purpose of which was to formally witness and document the creation of the CA's private signing keys. This helps assure the non-refutability of the integrity of the HKIRC Root CAs' key pairs, and in particular, the private signing keys.

HKIRC's management has securely generated key pairs, each consisting of a public and private key, in support of its CA operations. The key pairs were generated in accordance with procedures described in HKIRC's Certification Practice Statements (CPSs), and its Root Key Generation Script, which are in accordance with CA Key Generation Criterion 4.1 of the [WebTrust Principles and Criteria for Certification Authorities v2.2.3](#).

HKIRC's management established and maintained effective controls over the generation of these keys. These controls were designed to provide reasonable assurance of adherence to the above-mentioned practices throughout the root key generation process.

HKIRC's management is responsible for establishing and maintaining procedures over its CA root key generations, and over the integrity, confidentiality and availability of all private keys and access keys (including physical keys, tokens, and passwords) used in the establishment of the HKIRC Root CAs, and for the CA environment controls relevant to the generation and protection of its CA keys.

HKIRC uses Certizen Limited (“Certizen”) (subservice organization) to provide operation and maintenance services. The controls at Certizen, are necessary, in combination with controls at HKIRC, for HKIRC to achieve the applicable WebTrust Criteria as set out in the assertion. Certizen’s management assertion is presented following this assertion.

There are inherent limitations in any controls, including the possibility of human error, and the circumvention or overriding of controls. Accordingly, even effective controls can only provide reasonable assurance with respect that regarding the generation and protection of its CA keys. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

HKIRC’s management has assessed the procedures and controls for the generation of the CA keys. Based on that assessment, in HKIRC management’s opinion, in generating and protecting its CA keys for the HKIRC Root CAs on 15 September 2026, at Hong Kong Special Administrative Region of China, with the following identifying information:

Root Name	Subject Key Identifier	Certificate Serial Number
HKCA Root CA 3	CC1672E379FB74F2AF5F176F8B 44A1DC49EAA66C	31BE0C66A1EAEAACC4F3EFC4E5 E598FE7CD3BB6B
HKCA Root CA 4	A7106D800B50D411C40AA94DDC 350E463F2CE992	1FC8DE343A5BFAC64A2677A3EF9 6F1515F3B57EF
HKCA Root CA 5	5E12B37043EA17418D6456B9A0F C040044CD1D24	2103625EA3498B77C63E5F710E99 D4B61184D17E
HKCA Root CA 6	BA991D2FC1464179609FBFB387 241CAB71E9D15A	6ACBBF661D6E5D4D86F03D5DCD 975FFA211E36B3

HKIRC has:

- followed the CA key generation and protection requirements in its certification practice statements as enumerated in [Attachment A](#);
- included appropriate, detailed procedures and controls in its Root Key Generation Script:
 - HKCA S/MIME and Backup Root Key Generation Plan v3, 15 September 2026,
- maintained effective controls to provide reasonable assurance that the HKIRC Root CA keys were generated and protected in conformity with the procedures described in its CPS and its Root Key Generation Script;

- performed, during the root key generation process, all procedures required by the Root Key Generation Script;
- generated the CA keys in a physically secured environment as described in its CPS;
- generated the CA keys using personnel in trusted roles under multiple person control and split knowledge;
- generated the CA keys within cryptographic modules meeting the applicable technical and business requirements as disclosed in its CPS,

in accordance with CA Key Generation Criterion 4.1 of the [WebTrust Principles and Criteria for Certification Authorities v2.2.3](#).



Ir Wilson Wong

Chief Executive Officer of Hong Kong Internet Registration Corporation Limited

Hong Kong, 16 October 2026

Attachment A

The list of Certification Practice Statements in scope is as follows:

No.	Document Names
1	CPS for d-Cert (Personal) (Organisational) (Encipherment)
2	CPS for d-Cert (Server)
3	CPS for SMIME d-Cert (Personal) (Organisational) (Encipherment)
4	CPS for SMIME g-Cert

Certizen Limited Management's Assertion

Certizen Limited ("Certizen") provides operation and maintenance services to Hong Kong Internet Registration Corporation Limited ("HKIRC") who has deployed a public key infrastructure. As part of this deployment, it was necessary to create a hierarchy consistent of self-signed Root CAs known as HKCA Root CA 3, HKCA Root CA 4, HKCA Root CA 5 and HKCA Root CA 6 (collectively, "HKIRC Root CAs"). These CAs will serve as Root CAs for client certificate services. In order to allow the CAs to be installed in a final production configuration, a Root Key Generation Ceremony was conducted, the purpose of which was to formally witness and document the creation of the CA's private signing keys. This helps assure the non-refutability of the integrity of the HKIRC Root CAs' key pairs, and in particular, the private signing keys.

Certizen's management is responsible for establishing controls over its operations, to support HKIRC's CA root key generations, the integrity, confidentiality and availability of all private keys and access keys (including physical keys, tokens, and passwords) used in the establishment of the HKIRC Root CAs, and CA environment controls relevant to the generation and protection of HKIRC's CA keys.

There are inherent limitations in any controls, including the possibility of human error, and the circumvention or overriding of controls. Accordingly, even effective controls can only provide reasonable assurance with respect that regarding the generation and protection of HKIRC's CA keys. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

Certizen's management has assessed HKIRC's disclosure of its procedures and controls for the generation of the CA keys and Certizen's controls to provide operation and maintenance services to HKIRC in relation to the Root Key Generation Ceremony. Based on that assessment, in Certizen management's opinion, as HKIRC's independent subservice organization, in generating and protecting its CA keys for the HKIRC Root CAs on 15

September 2026, at Hong Kong Special Administrative Region of China, with the following identifying information:

Root Name	Subject Key Identifier	Certificate Serial Number
HKCA Root CA 3	CC1672E379FB74F2AF5F176F8 B44A1DC49EAA66C	31BE0C66A1EAEAACC4F3EF C4E5E598FE7CD3BB6B
HKCA Root CA 4	A7106D800B50D411C40AA94DD C350E463F2CE992	1FC8DE343A5BFAC64A2677A 3EF96F1515F3B57EF
HKCA Root CA 5	5E12B37043EA17418D6456B9A 0FC040044CD1D24	2103625EA3498B77C63E5F71 0E99D4B61184D17E
HKCA Root CA 6	BA991D2FC1464179609FBFB38 7241CAB71E9D15A	6ACBBF661D6E5D4D86F03D5 DCD975FFA211E36B3

Certizen has:

- followed the CA key generation and protection requirements in HKIRC's certification practice statements as enumerated in [Attachment A](#);
- included appropriate, detailed procedures and controls in HKIRC's Root Key Generation Script:
 - HKCA S/MIME and Backup Root Key Generation Plan v3, 15 September 2026,
- maintained effective controls to provide reasonable assurance that the HKIRC Root CA keys were generated and protected in conformity with the procedures described in HKIRC's CPS and Root Key Generation Script;
- performed, during the root key generation process, all procedures required by the Root Key Generation Script;
- generated the CA keys in a physically secured environment as described in HKIRC's CPS;
- generated the CA keys using personnel in trusted roles under multiple person control and split knowledge;
- generated the CA keys within cryptographic modules meeting the applicable technical and business requirements as disclosed in HKIRC's CPS,

in accordance with CA Key Generation Criterion 4.1 of the [WebTrust Principles and Criteria for Certification Authorities v2.2.3](#).



Eva Chan

Chief Executive Officer of Certizen Limited
Hong Kong, 16 October 2026

Attachment A

The list of Certification Practice Statements in scope is as follows:

No.	Document Names
1	CPS for d-Cert (Personal) (Organisational) (Encipherment)
2	CPS for d-Cert (Server)
3	CPS for SMIME d-Cert (Personal) (Organisational) (Encipherment)
4	CPS for SMIME g-Cert