pwc 羅兵咸永道

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 operating and maintenance services for the CA systems to HKIRC, that regarding the generation and protection of its HKCA Root CA 1 and HKCA Root CA 2 (collectively, "HKIRC Root CAs") on October 20, 2025, in the Hong Kong Special Administrative Region of the People's Republic of China, with the following identifying information:

Root Name	Subject Key Identifier	Certificate Serial Number
HKCA Root CA 1	eac79039365f0427584009f2bc1151178dc26c49	35705c45033058cc2caeb086c382234f49b57646
HKCA Root CA 2	1c6833e335b3fa57661b524da4b48737aa418fa9	06cafc8343591814b02e9432f7f3ffa5f11b3c5b

HKIRC and Certizen have:

- followed the CA key generation and protection requirements in Certification Practice Statement for d-Cert (Personal) (Organisational) (Encipherment) and Certification Practice Statement for d-Cert (Server);

- included appropriate, detailed procedures and controls in the HKCA Root Key Generation Plan v6, October 20, 2025;

- 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 CP/CPS and its Root Key Generation Script;

- performed, during the root key generation process, all procedures required by the Root Key Generation

PricewaterhouseCoopers, 22/F, Prince's Building, Central, Hong Kong
T: +852 2289 8888, F:+852 2810 9888, www.pwc.com/hk

Script;

- generated the CA keys in a physically secured environment as described in its CP/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 CP/CPS,

in accordance with CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.2.2.

HKIRC uses Certizen (subservice organization) to provide operating and maintenance services for the CA systems. The controls designed by HKIRC and operated by 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 the generation and protection of its CA keys in accordance with CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.2.2.

Subservice Organization's Responsibilities

Certizen has provided an accompanying assertion titled "Assertion of Certizen Management" (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 implementing, operating, and documenting controls designed 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 v2.2.2. 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 October 20, 2025 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.

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 October 20, 2025, 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 v2.2.2.

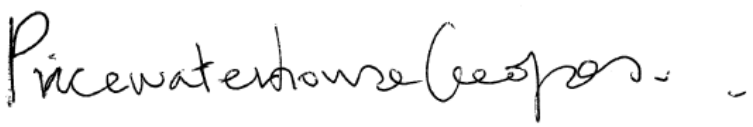
Emphasis of Matter

We draw attention to the fact that this report does not include any representation as to the quality of HKIRC and Certizen's services beyond those covered by CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.2.2, nor the suitability of any of HKIRC and Certizen's services for any customer's intended purpose. Our opinion is not modified in respect of this matter.

Purpose and Restriction on Use

The assertions were prepared for use in connection and for submitting root inclusion request to major browser vendors using CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.2.2 designed for this purpose. As a result, the assertions may not be suitable for another purpose. This report is intended solely for the management of HKIRC in connection with submitting root inclusion request to major browser vendors in connection with CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.2.2.

Our report is not to be used for any other purpose. We do not assume responsibility towards or accept liability to any other parties for the contents of this report.



PricewaterhouseCoopers

Certified Public Accountants

Hong Kong, November 28, 2025

Hong Kong Internet Registration Corporation Limited

Hong Kong Internet Registration Corporation Limited
Unit 501, Level 5, Core C, Cyberport 3,
100 Cyberport Road, Hong Kong
Tel: (852) 2319 2303
Fax: (852) 2319 2626
Email: info@hkirc.hk
https://www.hkirc.hk

PricewaterhouseCoopers
22/F, Prince's Building, Central, Hong Kong

November 28, 2025

Dear Sirs,

Assertion by Management as to the Disclosure of Business Practices and Controls over Hong Kong Internet Registration Corporation Limited ("HKIRC") - Root Key Generation Ceremony on October 20, 2025

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 1 and HKCA Root CA 2 (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 key. 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 Certificate Policy (CP) and Certification Practice Statement (CPS), 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 v2.2.2.

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 effective controls 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 operating and maintenance services for the CA systems. The controls designed by HKIRC and operated by Certizen, are necessary, in combination with controls at HKIRC, for HKIRC to achieve the applicable WebTrust Criteria as set out in HKIRC's 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 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 management's opinion, that regarding the generation and protection its CA keys for the HKIRC Root CAs on October 20, 2025, at Hong Kong Special Administrative Region of the People's Republic of China, with the following identifying information:

Root Name	Subject Key Identifier	Certificate Serial Number
HKCA Root CA 1	eac79039365f0427584009f2bc1151178dc26c49	35705c45033058cc2caeb086c382234f49b57646
HKCA Root CA 2	1c6833e335b3fa57661b524da4b48737aa418fa9	06cafc8343591814b02e9432f7f3ffa5f11b3c5b

HKIRC has:

- followed the CA key generation and protection requirements in its:
  - Certification Practice Statement for d-Cert (Personal) (Organisational) (Encipherment);
  - Certification Practice Statement for d-Cert (Server)

- included appropriate, detailed procedures and controls in its Root Key Generation Script:
  - HKCA Root Key Generation Plan v6, October 20, 2025,

- 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 CP/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 CP/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 CP/CPS,

in accordance with CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.2.2.

Ir Wilson Wong
Chief Executive Officer of Hong Kong Internet Registration Corporation Limited

Certizen Limited

Certizen Limited
Units 908-915, L9, Core F, Cyberport 3,
100 Cyberport Road, Hong Kong
Tel: (852) 2121 2121
Email: info@certizen.com
https://www.certizen.com/

PricewaterhouseCoopers
22/F, Prince's Building, Central, Hong Kong

November 28, 2025

Dear Sirs,

Assertion by Management as to the Disclosure of Business Practices and Controls over Hong Kong Internet Registration Corporation Limited ("HKIRC") with Certizen Limited ("Certizen") as its subservice organization - Root Key Generation Ceremony on October 20, 2025

Certizen provides operating and maintenance service for the CA systems to 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 1 and HKCA Root CA 2 (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 key. 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 operating controls designed by HKIRC 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 operating and maintenance service for the CA systems 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, that regarding the generation and protection of in Hong Kong Special Administrative Region of the People's Republic of China on October 20, 2025, with the following identifying information:

Root Name	Subject Key Identifier	Certificate Serial Number
HKCA Root CA 1	eac79039365f0427584009f2bc1151178dc26c49	35705c45033058cc2caeb086c382234f49b57646
HKCA Root CA 2	1c6833e335b3fa57661b524da4b48737aa418fa9	06cafc8343591814b02e9432f7f3ffa5f11b3c5b

Certizen has:

- followed the CA key generation and protection requirements in HKIRC's:
  - Certification Practice Statement for d-Cert (Personal) (Organisational) (Encipherment);
  - Certification Practice Statement for d-Cert (Server),

- included appropriate, detailed procedures and controls in HKIRC's Root Key Generation Script:
  - HKCA Root Key Generation Plan v6, October 20, 2025,

- 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 CP/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 CP/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 CP/CPS,

in accordance with CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.2.2.

Eva Chan
Chief Executive Officer of Certizen Limited