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 accompanying 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 for its Certification Authority ("CA") operations at locations as enumerated in Attachment A, for the period from 20 October 2025 to 25 June 2026 for its CAs as enumerated in Attachment B, HKIRC with Certizen as its subservice organization has:

- disclosed its TLS certificate lifecycle management business practices in its certification practice statements as enumerated in Attachment C, including its commitment to provide TLS certificates in conformity with the CA/Browser Forum Requirements on the HKIRC website, and provided such services in accordance with its disclosed practices,

- maintained effective controls to provide reasonable assurance that:

  - the integrity of keys and TLS certificates it manages is established and protected throughout their lifecycles; and

  - TLS subscriber information is properly authenticated (for the registration activities performed by HKIRC with Certizen as its subservice organization),

- maintained effective controls to provide reasonable assurance that:

  - logical and physical access to CA systems and data is restricted to authorized individuals;

  - the continuity of key and certificate management operations is maintained; and

  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity,

in accordance with the WebTrust Principles and Criteria for Certification Authorities – TLS Baseline v2.2.5.

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

The CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates require the CA to operate controls to adhere to the Network and Certificate System Security Requirements. The WebTrust Principles and Criteria for Certification Authorities – Network Security address this requirement and are reported on in a separate report.

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 the management's assertion, including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities – TLS Baseline v2.2.5.

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 designing, 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 as 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 WebTrust Principles and Criteria for Certification Authorities – TLS Baseline v2.2.5. 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 TLS certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of TLS certificates; (2) selectively testing transactions executed in accordance with disclosed TLS certificate lifecycle management business practices; (3) testing and evaluating the operating effectiveness of the controls; and (4) 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, throughout the period 20 October 2025 to 25 June 2026, the assertions by the management of HKIRC and Certizen, as referred to above, are fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities – TLS Baseline v2.2.5.

This report does not include any representation as to the quality of HKIRC and Certizen's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – TLS Baseline v2.2.5, nor the suitability of any of HKIRC and Certizen's services for any customer's intended purpose.

Other Matter

As indicated in the assertions by the management of HKIRC and Certizen, HKIRC with Certizen as its subservice organization began issuing subscriber certificates only after the Commissioner for Digital Policy ("CDP") granted recognition to HKIRC as a recognized Certification Authority on 16 April 2026. No subscriber certificates were issued during the period from 20 October 2025 to 16 April 2026. Therefore, we did not perform any tests of the operating effectiveness of controls related to the WebTrust principle and criteria "The Certification Authority ("CA") maintains effective controls to provide reasonable assurance that Subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority ("RA") and subcontractor) and verified" and accordingly, we do not express an opinion on the operating effectiveness of controls to achieve this WebTrust principle and criteria during the period from 20 October 2025 to 16 April 2026.

Use of the WebTrust seal

HKIRC's use of the WebTrust for Certification Authorities – TLS Baseline Seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

PricewaterhouseCoopers

Certified Public Accountants

Hong Kong, 17 July 2026

4 The maintenance and integrity of the HKIRC website is the responsibility of the management of HKIRC; the work carried out by the assurance provider does not involve consideration of these matters and, accordingly, the assurance provider accepts no responsibility for any differences between the accompanying management's assertion of HKIRC on which the assurance report was issued or the assurance report that was issued and the information presented on the website.

Attachment A

The list of CA locations in scope for the period from 20 October 2025 to 25 June 2026 is as follow:

Location Name	Location	In-Scope for Physical and Environmental Control Testing
Facility 1	Hong Kong Special Administrative Region of the People's Republic of China	Yes
Facility 2	Hong Kong Special Administrative Region of the People's Republic of China	Yes

Attachment B

The list of CAs and certificates in scope for the period from 20 October 2025 to 25 June 2026 is as follow:

Root CA

CA #	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	SKI	SHA256 Fingerprint
1	1	CN=HKCA Root CA 2 O=Hong Kong Internet Registration Corporation Limited L=Hong Kong ST=Hong Kong C=HK	CN=HKCA Root CA 2 O=Hong Kong Internet Registration Corporation Limited L=Hong Kong ST=Hong Kong C=HK	06CAFC8343591814B02E9432F7F3FFA5F11B3C5B	rsaEncryption	(4096 Bits)	sha256WithRSAEncryption	1C6833E335B3FA57661B524DA4B48737AA418FA9	98900822A3D6A97BD8310D0570F1E6A551B6B8356FFE3D4E8258238E2286C06A

Sub CA

CA #	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	SKI	SHA256 Fingerprint
1	1	CN=HKCA d-Cert DV SSL CA 2 - 25 O=Hong Kong Internet Registration Corporation Limited L=Hong Kong ST=Hong Kong C=HK	CN=HKCA Root CA 2 O=Hong Kong Internet Registration Corporation Limited L=Hong Kong ST=Hong Kong C=HK	30995EC319A8C8335AA75E9FDD12FE1C18AAFBD6	rsaEncryption	(2048 Bits)	sha256WithRSAEncryption	63E458303B08E716DCAA7D81DFF7988CEC2C1C9A	6CB01D5B11201C5E5DBDE2EB0A45D400AEF3FF5EEF639076B9E8382DF3B79269
2	1	CN=HKCA d-Cert OV SSL CA 2 - 25 O=Hong Kong Internet Registration Corporation Limited L=Hong Kong ST=Hong Kong	CN=HKCA Root CA 2 O=Hong Kong Internet Registration Corporation Limited L=Hong Kong ST=Hong Kong C=HK	5CA4C51C0F85BA969B728CC25FF17CC9D068D07F	rsaEncryption	(2048 Bits)	sha256WithRSAEncryption	87404AFBDDCD2A406EFC0B00695B96729CC90261	C5F48839B21494A1169D36FB0C52D198FD3F62DF1D2E2179E0941E4FB6084152

CA #	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	SKI	SHA256 Fingerprint
		C=HK							
3	1	CN=HKCA d-Cert EV SSL CA 2 - 25 O=Hong Kong Internet Registration Corporation Limited L=Hong Kong ST=Hong Kong C=HK	CN=HKCA Root CA 2 O=Hong Kong Internet Registration Corporation Limited L=Hong Kong ST=Hong Kong C=HK	7C8A89A56A845332FAD3B22FF649814180BFFDE7	rsaEncryption	(2048 Bits)	sha256WithRSAEncryption	B4E2B7CD19104FB1E81E0774B073E06644448C8C	977BCED89D7B83751D650EC3B6FD9472B713B23B8EC1FCEC0F966D53677E445E

Attachment C

The list of HKIRC's Certification Practice Statements in scope for the period from 20 October 2025 to 25 June 2026 is as follow:

Document Names	Version
CPS for d-Cert (Server)	OID = 1.3.6.1.4.1.64092.1.7.1 (Effective from 16 April 2026)

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

Hong Kong Internet Registration Corporation Limited ("HKIRC") operates the Certification Authority ("CA") services for its CAs as enumerated in Attachment A, and provides TLS CA services.

The management of HKIRC is responsible for establishing and maintaining effective controls over its TLS CA operations, including its TLS CA business practices disclosure on its website, TLS key lifecycle management controls, and TLS certificate lifecycle management controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

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 to HKIRC's Certification Authority operations.

HKIRC management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in HKIRC management's opinion, in providing its TLS CA services in the Hong Kong Special Administrative Region of the People's Republic of China (including Facility 1 and Facility 2), throughout the period 20 October 2025 to 25 June 2026, HKIRC has:

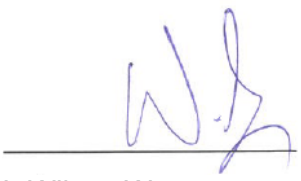
- disclosed its TLS certificate lifecycle management business practices in its certification practice statements as enumerated in Attachment B, including its commitment to provide TLS certificates in conformity with the CA/Browser Forum Requirement on the HKIRC website, and provided such services in accordance with its disclosed practices,

- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and TLS certificates it manages is established and protected throughout their lifecycles; and
  - TLS subscriber information is properly authenticated (for the registration activities performed by HKIRC with Certizen as its subservice organization),

- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorized individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity,

in accordance with the WebTrust Principles and Criteria for Certification Authorities – TLS Baseline v2.2.5.

HKIRC with Certizen as its subservice organization began issuing subscriber certificates only after the Commissioner for Digital Policy (CDP) granted recognition to HKIRC as a recognized Certification Authority on 16 April 2026. As no subscriber certificates were issued during the period from October 20, 2025, to April 16, 2026, the controls related to the WebTrust principles and criteria "The Certification Authority (CA) maintains effective controls to provide reasonable assurance that Subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified" did not operate during the period from October 20, 2025, to April 16, 2026.



Ir Wilson Wong
Chief Executive Officer of Hong Kong Internet Registration Corporation Limited
Hong Kong, 17 July 2026

Attachment A

The list of CAs and certificates covered in the management's assertion for the period from 20 October 2025 to 25 June 2026 is as follow:

Root CAs

CA #	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	SKI	SHA256 Fingerprint
1	1	CN=HKCA Root CA 2 O=Hong Kong Internet Registration Corporation Limited L=Hong Kong ST=Hong Kong C=HK	CN=HKCA Root CA 2 O=Hong Kong Internet Registration Corporation Limited L=Hong Kong ST=Hong Kong C=HK	06CAFC8343591814B02E9432F7F3FFA5F11B3C5B	rsaEncryption	(4096 Bits)	sha256WithRSAEncryption	1C6833E335B3FA57661B524DA4B48737AA418FA9	98900822A3D6A97BD8310D0570F1E6A551B6B8356FFE3D4E8258238E2286C06A

Sub CAs

CA #	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	SKI	SHA256 Fingerprint
1	1	CN=HKCA d-Cert DV SSL CA 2 - 25 O=Hong Kong Internet Registration Corporation Limited L=Hong Kong ST=Hong Kong C=HK	CN=HKCA Root CA 2 O=Hong Kong Internet Registration Corporation Limited L=Hong Kong ST=Hong Kong C=HK	30995EC319A8C8335AA75E9FDD12FE1C18AAFBD6	rsaEncryption	(2048 Bits)	sha256WithRSAEncryption	63E458303B08E716DCAA7D81DFF7988CEC2C1C9A	6CB01D5B11201C5E5DBDE2EB0A45D400AEF3FF5EEF639076B9E8382DF3B79269
2	1	CN=HKCA d-Cert OV SSL CA 2 - 25 O=Hong Kong Internet Registration Corporation Limited L=Hong Kong ST=Hong Kong C=HK	CN=HKCA Root CA 2 O=Hong Kong Internet Registration Corporation Limited L=Hong Kong ST=Hong Kong C=HK	5CA4C51C0F85BA969B728CC25FF17CC9D068D07F	rsaEncryption	(2048 Bits)	sha256WithRSAEncryption	87404AFBDDCD2A406EFC0B00695B96729CC90261	C5F48839B21494A1169D36FB0C52D198FD3F62DF1D2E2179E0941E4FB6084152

CA #	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	SKI	SHA256 Fingerprint
3	1	CN=HKCA d-Cert EV SSL CA 2 - 25 O=Hong Kong Internet Registration Corporation Limited L=Hong Kong ST=Hong Kong C=HK	CN=HKCA Root CA 2 O=Hong Kong Internet Registration Corporation Limited L=Hong Kong ST=Hong Kong C=HK	7C8A89A56A845332FAD3B22FF649814180BFFDE7	rsaEncryption	(2048 Bits)	sha256WithRSAEncryption	B4E2B7CD19104FB1E81E0774B073E06644448C8C	977BCED89D7B83751D650EC3B6FD9472B713B23B8EC1FCEC0F966D53677E445E

Attachment B

The list of HKIRC's Certification Practice Statements covered in the management's assertion for the period from 20 October 2025 to 25 June 2026 is as follow:

Document Names	Version
CPS for d-Cert (Server)	OID = 1.3.6.1.4.1.64092.1.7.1 (Effective from 16 April 2026)

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/

Certizen Limited ("Certizen") provides operation and maintenance services for Hong Kong Internet Registration Corporation Limited ("HKIRC"), who operates the Certification Authority ("CA") services and provides TLS CA services for the CAs enumerated in Attachment A.

The management of Certizen is responsible for establishing and maintaining effective controls over its operations, to support HKIRC's TLS CA operations, including HKIRC's TLS CA business practices disclosure on its website, TLS key lifecycle management controls, and TLS certificate lifecycle management controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

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 to supporting HKIRC's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

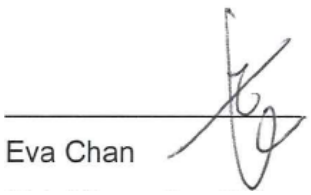
Certizen's management has assessed HKIRC's disclosure of its certificate practice and Certizen's controls to provide operation and maintenance services for HKIRC in relation to TLS CA services. Based on that assessment, in Certizen management's opinion, as HKIRC's independent subservice organization, in providing operation and maintenance services for HKIRC in Hong Kong Special Administrative Region of the People's Republic of China (including Facility 1 and Facility 2), throughout the period 20 October 2025 to 25 June 2026, Certizen has:

- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and TLS certificates it manages is established and protected throughout their lifecycles; and
  - TLS subscriber information is properly authenticated (for the registration activities performed by HKIRC with Certizen as its subservice organization);

- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorized individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity,

in accordance with the WebTrust Principles and Criteria for Certification Authorities – TLS Baseline v2.2.5.

HKIRC with Certizen as its subservice organization began issuing subscriber certificates only after the Commissioner for Digital Policy (CDP) granted recognition to HKIRC as a recognized Certification Authority on 16 April 2026. As no subscriber certificates were issued during the period from October 20, 2025, to April 16, 2026, the controls related to the WebTrust principles and criteria "The Certification Authority (CA) maintains effective controls to provide reasonable assurance that Subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified" did not operate during the period from October 20, 2025, to April 16, 2026.



Eva Chan
Chief Executive Officer of Certizen Limited
Hong Kong, 17 July 2026

Attachment A

The list of CAs and certificates covered in the management's assertion for the period from 20 October 2025 to 25 June 2026 is as follow:

Root CAs

CA #	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	SKI	SHA256 Fingerprint
1	1	CN=HKCA Root CA 2 O=Hong Kong Internet Registration Corporation Limited L=Hong Kong ST=Hong Kong C=HK	CN=HKCA Root CA 2 O=Hong Kong Internet Registration Corporation Limited L=Hong Kong ST=Hong Kong C=HK	06CAFC8343591814B02E9432F7F3FFA5F11B3C5B	rsaEncryption	(4096 Bits)	sha256WithRSAEncryption	1C6833E335B3FA57661B524DA4B48737AA418FA9	98900822A3D6A97BD8310D0570F1E6A551B6B8356FFE3D4E8258238E2286C06A

Sub CAs

CA #	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	SKI	SHA256 Fingerprint
1	1	CN=HKCA d-Cert DV SSL CA 2 - 25 O=Hong Kong Internet Registration Corporation Limited L=Hong Kong ST=Hong Kong C=HK	CN=HKCA Root CA 2 O=Hong Kong Internet Registration Corporation Limited L=Hong Kong ST=Hong Kong C=HK	30995EC319A8C8335AA75E9FDD12FE1C18AAFBD6	rsaEncryption	(2048 Bits)	sha256WithRSAEncryption	63E458303B08E716DCAA7D81DFF7988CEC2C1C9A	6CB01D5B11201C5E5DBDE2EB0A45D400AEF3FF5EEF639076B9E8382DF3B79269
2	1	CN=HKCA d-Cert OV SSL CA 2 - 25 O=Hong Kong Internet Registration Corporation Limited L=Hong Kong ST=Hong Kong C=HK	CN=HKCA Root CA 2 O=Hong Kong Internet Registration Corporation Limited L=Hong Kong ST=Hong Kong C=HK	5CA4C51C0F85BA969B728CC25FF17CC9D068D07F	rsaEncryption	(2048 Bits)	sha256WithRSAEncryption	87404AFBDDCD2A406EFC0B00695B96729CC90261	C5F48839B21494A1169D36FB0C52D198FD3F62DF1D2E2179E0941E4FB6084152

CA #	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	SKI	SHA256 Fingerprint
3	1	CN=HKCA d-Cert EV SSL CA 2 - 25 O=Hong Kong Internet Registration Corporation Limited L=Hong Kong ST=Hong Kong C=HK	CN=HKCA Root CA 2 O=Hong Kong Internet Registration Corporation Limited L=Hong Kong ST=Hong Kong C=HK	7C8A89A56A845332FAD3B22FF649814180BFFDE7	rsaEncryption	(2048 Bits)	sha256WithRSAEncryption	B4E2B7CD19104FB1E81E0774B073E06644448C8C	977BCED89D7B83751D650EC3B6FD9472B713B23B8EC1FCEC0F966D53677E445E