pwc 羅兵咸永道

Independent Practitioner's assurance report

To the Management of Hongkong Post Certification Authority:

Scope

We have been engaged to perform a reasonable assurance engagement on the accompanying management's assertion of Hongkong Post Certification Authority ("HKPCA") with Certizen Limited ("Certizen") as its agent in providing its Certification Authority ("CA") operations in the Hong Kong Special Administrative Region of the People's Republic of China for the period from 1 December 2023 to 30 November 2024 for its CAs as enumerated in Appendix C, HKPCA with Certizen as its agent has:

- disclosed its extended validation SSL ("EV SSL") certificate lifecycle management business practices in its Certification Practice Statements ("CPS"), including its commitment to provide EV SSL certificates referenced in Appendix D in conformity with the CA/Browser Forum Guidelines on the HKPCA's website, and provided such services in accordance with its disclosed practices,

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

in accordance with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.8.

Management's Responsibilities

The management of HKPCA with Certizen as its agent 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 – Extended Validation SSL v1.8.

Our Independence and Quality Management

We have complied with the independence and other ethical requirements of the International Code of Ethics for Professional Accountants (including International Independence Standards) issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

Our firm applies International Standard on Quality Management 1, 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 management's assertion based on our work performed.

We conducted our procedures in accordance with International Standard on Assurance Engagements 3000 (Revised) "Assurance Engagements Other Than Audits or Reviews of Historical Financial Information", issued by the International Auditing and Assurance Standards Board. 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 management's assertion of HKPCA (with Certizen as its agent) is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.8. 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:

- obtaining an understanding of HKPCA's EV SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of EV SSL certificates;
- selectively testing transactions executed in accordance with disclosed EV SSL certificate lifecycle management practices;
- testing and evaluating the operating effectiveness of the controls; and
- performing such other procedures as we considered necessary in the circumstances.

The relative effectiveness and significance of specific controls at HKPCA 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, HKPCA (with Certizen as its agent)'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, the management's assertion of HKPCA with Certizen as its agent, for the period from 1 December 2023 to 30 November 2024, is fairly stated, in all material respects, in

accordance with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.8.

Emphasis of Matter

This report does not include any representation as to the quality of HKPCA (with Certizen as its agent)'s services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.8, nor the suitability of any of HKPCA (with Certizen as its agent)'s services for any customer's intended purpose.

Our opinion is not modified in respect of this matter.

Other Matter

We noted the following other matter during our procedures:

HKPCA's management has disclosed five incidents (see Appendix B) during the period from 1 December 2023 to 30 November 2024. The remedial actions and the root causes of these incidents undertaken by HKPCA have been posted publicly in the online forums of the Bugzilla site, as well as the online forums of individual internet browsers that comprise the CA/Browser Forum.

Our opinion is not modified in respect of this matter.

Purpose and Restriction on Use

The management's assertion was prepared for obtaining and displaying the WebTrust Seal on HKPCA website[1] using WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.8 designed for this purpose. As a result, the management's assertion of HKPCA (with Certizen as its agent) may not be suitable for another purpose. This report is intended solely for management of HKPCA in connection with obtaining and displaying the WebTrust Seal on its website after submitting the report to the related authority in connection with WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.8.

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.

[1] *The maintenance and integrity of the HKPCA website is the responsibility of the Management of HKPCA; 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 HKPCA on which the assurance report was issued or the assurance report that was issued and the information presented on the website.*

Use of the WebTrust seal

HKPCA's use of the WebTrust for Certification Authorities – Extended Validation SSL 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, 24 February 2025

Appendix A – Auditor's information

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

Appendix B – Publicly disclosed incidents during the period from 1 December 2023 to 30 November 2024

Bugzilla ID	Disclosure	Publicly Disclosed Link
1887888	Hongkong Post: Delayed revocation of TLS certificates with basicConstraints not marked as critical	Bugzilla Ticket Link
1887008	Hongkong Post: TLS certificates with basicConstraints not marked as critical	Bugzilla Ticket Link
1886722	Hongkong Post: Delayed response to CPR	Bugzilla Ticket Link
1886665	Hongkong Post: Delayed revocation of TLS certificates with Certificate Policies extension problem	Bugzilla Ticket Link
1886406	Hongkong Post: TLS certificates with Certificate Policies extension that does not assert http scheme	Bugzilla Ticket Link

Appendix C – In Scope CA

List of HKPCA's Root CA:

Reference	Root CA Name	Remarks
1	Hongkong Post Root CA 3	Valid from 3 June 2017
Subject DN C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post Root CA 3 SHA-1 Thumbprint 58A2D0EC2052815BC1F3F86402244EC28E024B02 SHA-256 Thumbprint 5A2FC03F0C83B090BBFA40604B0988446C7636183DF9846E17101A447FB8EFD6		

List of HKPCA's Subordinate CA:

Reference	Subordinate CA Name	Remarks
1	Hongkong Post e-Cert SSL CA 3 - 17	Valid from 3 June 2017 for issuance of non-EV SSL certificate
Subject DN C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post e-Cert SSL CA 3 - 17 SHA-1 Thumbprint 92797871DC6A0B6EE1417BB657D7ED6FC6F975EB SHA-256 Thumbprint 69ECDBC3147F581DFDCB522D9DEFB260B26784AD4955C74E6A52522CCC4C4408		
2	Hongkong Post e-Cert EV SSL CA 3 - 17	Valid from 3 June 2017 for issuance of EV SSL certificate
Subject DN C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post e-Cert EV SSL CA 3 - 17 SHA-1 Thumbprint 6CA9BB1B3BAEF67D6D5414132A7EFB212836639E SHA-256 Thumbprint C18D53BF9864DD09BCBCACFD672E2566D4C81F6889E36DF5DD425C04211D0763		

3	Hongkong Post Root CA 3	Cross certificate signed by Hongkong Post Root CA 1 and revoked on 12 August 2017
Subject DN C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post Root CA 3 SHA-1 Thumbprint D0D535192598FCA8B68789EDCEF1EA51B3A898A5 SHA-256 Thumbprint ABFA404ECEEA854381ABE294AC829440E0133E077911A67E1293CF111AC43C44		
4	Hongkong Post Root CA 3	Cross certificate signed by Hongkong Post Root CA 1 and valid from 12 August 2017 and expired on 15 May 2023
Subject DN C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post Root CA 3 SHA-1 Thumbprint 97FC47E174E2AA5332321DCFF6077A19F04387F0 SHA-256 Thumbprint 176AEBF2972BD6F47179EDE3DE63848B1543B45AE2954BEA45185B152537B9C4		
5	Hongkong Post Root CA 3	Cross certificate signed by Hongkong Post Root CA 1 and revoked on 27 July 2022
Subject DN C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post Root CA 3 SHA-1 Thumbprint 881700C3346CBA89A8C1C5C44A584A8441319944 SHA-256 Thumbprint F8F6037491861C069D3BB442B78A3DB4049EE7787B7C2841A7BA6966B5272F2C		

6	Hongkong Post Root CA 3	Cross certificate signed by Hongkong Post Root CA 1 and valid from 27 July 2022 and expired on 15 May 2023
Subject DN C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post Root CA 3 SHA-1 Thumbprint 3069BCFC8DD0AFBAABA5CA81D23CCC6413131F6F SHA-256 Thumbprint 5544A24FEB21F681F1987D30E0AF5C49E9F9FFFD5550A889B40B1EC9CC81E667		
7	Hongkong Post Root CA 3	Cross-certificate issued by GlobalSign root CA "GlobalSign Root CA - R3" and valid from 16 November 2022 to establish a trust relationship from Hongkong Post Root CA 3 to GlobalSign Root CA - R3
Subject DN C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post Root CA 3 SHA-1 Thumbprint AF0F1F7AFBD02E3DDE39BD0B646CF97B7D122408 SHA-256 Thumbprint 00482341B104A0DE6E0F1D508DB84CB514F7494FE04982133A5C750136C55DC8		

Appendix D - List of HKPCA's Certification Practice Statements

Document Names	Version
CPS for e-Cert (Server)	OID = 1.3.6.1.4.1.16030.1.7.18 (valid from 15 September 2023) OID = 1.3.6.1.4.1.16030.1.7.19 (valid from 21 December 2023) OID = 1.3.6.1.4.1.16030.1.7.20 (valid from 22 March 2024) OID = 1.3.6.1.4.1.16030.1.7.21 (valid from 25 July 2024) OID = 1.3.6.1.4.1.16030.1.7.22 (valid from 15 August 2024) ^

^ Latest CPS version

PricewaterhouseCoopers
22/F Prince's Building
Central
Hong Kong

24 February 2025

Dear Sirs,

Assertion by Management as to the Disclosure of Business Practices and Controls over the Hongkong Post Certification Authority EV SSL Certification Authority Services during the period from 1 December 2023 to 30 November 2024

The Postmaster General operates the Certification Authority ("CA") services known as Hongkong Post Certification Authority ("HKPCA") through its Root CAs and Subordinate CAs referenced in Appendix A and provides Extended Validation SSL ("EV SSL") CA services.

The management of HKPCA with Certizen Limited ("Certizen") as its agent is responsible for establishing and maintaining effective controls over its EV SSL CA operations, including its EV SSL CA business practices disclosure on its website, EV SSL key lifecycle management controls, and EV SSL 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 HKPCA's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

The management of HKPCA with Certizen as its agent has assessed its disclosures of its certificate practices and controls over its EV SSL CA services. Based on that assessment, in management's opinion, HKPCA with Certizen as its agent, in providing its EV SSL CA services in the Hong Kong Special Administrative Region of the People's Republic of China, throughout the period from 1 December 2023 to 30 November 2024, HKPCA with Certizen as its agent has:

- disclosed its EV SSL certificate lifecycle management business practices in its Certification Practice Statements ("CPS"), including its commitment to provide EV SSL certificates referenced in Appendix B in conformity with the CA/Browser Forum Guidelines on the HKPCA website, and provided such services in accordance with its disclosed practices,
- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and EV SSL certificates it manages is established and protected throughout their lifecycles; and

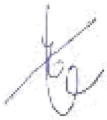
– EV SSL subscriber information is properly collected, authenticated (for the registration activities performed by HKPCA with Certizen as its agent),

in accordance with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.8.

HKPCA has disclosed five incidents (see Appendix C) during the period from 1 December 2023 to 30 November 2024. The remedial actions and the root causes of these incidents undertaken by HKPCA have been posted publicly in the online forums of the Bugzilla site, as well as the online forums of individual internet browsers that comprise the CA/Browser Forum.

Yours faithfully,

(Lilian MAK)
for Postmaster General



(Eva CHAN)
for Certizen Limited

Appendix A

List of HKPCA's Root CA:

Reference	Root CA Name	Remarks
1	Hongkong Post Root CA 3	Valid from 3 June 2017
Subject DN C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post Root CA 3 SHA-1 Thumbprint 58A2D0EC2052815BC1F3F86402244EC28E024B02 SHA-256 Thumbprint 5A2FC03F0C83B090BBFA40604B0988446C7636183DF9846E17101A447FB8EFD6		

List of HKPCA's Subordinate CA:

Reference	Subordinate CA Name	Remarks
1	Hongkong Post e-Cert SSL CA 3 - 17	Valid from 3 June 2017 for issuance of non-EV SSL certificate
Subject DN C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post e-Cert SSL CA 3 - 17 SHA-1 Thumbprint 92797871DC6A0B6EE1417BB657D7ED6FC6F975EB SHA-256 Thumbprint 69ECDBC3147F581DFDCB522D9DEFB260B26784AD4955C74E6A52522CCC4C4408		
2	Hongkong Post e-Cert EV SSL CA 3 - 17	Valid from 3 June 2017 for issuance of EV SSL certificate
Subject DN C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post e-Cert EV SSL CA 3 - 17 SHA-1 Thumbprint 6CA9BB1B3BAEF67D6D5414132A7EFB212836639E SHA-256 Thumbprint C18D53BF9864DD09BCBCACFD672E2566D4C81F6889E36DF5DD425C04211D0763		

3	Hongkong Post Root CA 3	Cross certificate signed by Hongkong Post Root CA 1 and revoked on 12 August 2017
Subject DN C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post Root CA 3 SHA-1 Thumbprint D0D535192598FCA8B68789EDCEF1EA51B3A898A5 SHA-256 Thumbprint ABFA404ECEEA854381ABE294AC829440E0133E077911A67E1293CF111AC43C44		
4	Hongkong Post Root CA 3	Cross certificate signed by Hongkong Post Root CA 1 and valid from 12 August 2017 and expired on 15 May 2023
Subject DN C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post Root CA 3 SHA-1 Thumbprint 97FC47E174E2AA5332321DCFF6077A19F04387F0 SHA-256 Thumbprint 176AEBF2972BD6F47179EDE3DE63848B1543B45AE2954BEA45185B152537B9C4		
5	Hongkong Post Root CA 3	Cross certificate signed by Hongkong Post Root CA 1 and revoked on 27 July 2022
Subject DN C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post Root CA 3 SHA-1 Thumbprint 881700C3346CBA89A8C1C5C44A584A8441319944 SHA-256 Thumbprint F8F6037491861C069D3BB442B78A3DB4049EE7787B7C2841A7BA6966B5272F2C		

6	Hongkong Post Root CA 3	Cross certificate signed by Hongkong Post Root CA 1 and valid from 27 July 2022 and expired on 15 May 2023
Subject DN C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post Root CA 3 SHA-1 Thumbprint 3069BCFC8DD0AFBAABA5CA81D23CCC6413131F6F SHA-256 Thumbprint 5544A24FEB21F681F1987D30E0AF5C49E9F9FFFD5550A889B40B1EC9CC81E667		
7	Hongkong Post Root CA 3	Cross-certificate issued by GlobalSign root CA "GlobalSign Root CA - R3" and valid from 16 November 2022 to establish a trust relationship from Hongkong Post Root CA 3 to GlobalSign Root CA - R3
Subject DN C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post Root CA 3 SHA-1 Thumbprint AF0F1F7AFBD02E3DDE39BD0B646CF97B7D122408 SHA-256 Thumbprint 00482341B104A0DE6E0F1D508DB84CB514F7494FE04982133A5C750136C55DC8		

Appendix B

List of HKPCA's Certification Practice Statements

Document Names	Version
CPS for e-Cert (Server)	OID = 1.3.6.1.4.1.16030.1.7.18 (valid from 15 September 2023) OID = 1.3.6.1.4.1.16030.1.7.19 (valid from 21 December 2023) OID = 1.3.6.1.4.1.16030.1.7.20 (valid from 22 March 2024) OID = 1.3.6.1.4.1.16030.1.7.21 (valid from 25 July 2024) OID = 1.3.6.1.4.1.16030.1.7.22 (valid from 15 August 2024) ^

^ Latest CPS version

Appendix C

Publicly disclosed incidents

Bugzilla ID	Disclosure	Publicly Disclosed Link
1887888	Hongkong Post: Delayed revocation of TLS certificates with basicConstraints not marked as critical	Bugzilla Ticket Link
1887008	Hongkong Post: TLS certificates with basicConstraints not marked as critical	Bugzilla Ticket Link
1886722	Hongkong Post: Delayed response to CPR	Bugzilla Ticket Link
1886665	Hongkong Post: Delayed revocation of TLS certificates with Certificate Policies extension problem	Bugzilla Ticket Link
1886406	Hongkong Post: TLS certificates with Certificate Policies extension that does not assert http scheme	Bugzilla Ticket Link