

Independent Practitioner’s assurance report

To 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 for its extended validation SSL (“EV SSL”) Certification Authority (“CA”) operations in the Hong Kong Special Administrative Region of the People’s Republic of China for the period from 1 December 2022 to 30 November 2023 for its CAs enumerated in [Appendix C](#), 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 D](#) in conformity with the CA/Browser Forum Guidelines and provided such services in accordance with its CPS; and
- 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) and verified,

in accordance with the [WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.8](#).

Management’s Responsibilities

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 Control

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 Control 1 issued by the HKICPA and accordingly maintains a comprehensive system of quality control including documented policies and 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 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 HKICPA¹. 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 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 key and certificate lifecycle management business practices and its controls over EV SSL key and certificate integrity, over the authenticity and confidentiality of subscriber and relying party information, over the continuity of EV SSL key and certificate lifecycle management operations and over development, maintenance and operation of systems integrity;
- selectively testing transactions executed in accordance with disclosed key and certificate lifecycle management business 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 subscribers and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscribers 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’s ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct error, fraud, unauthorized 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, for the period from 1 December 2022 to 30 November 2023, is fairly stated, in all material respects, in accordance with the [WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.8](#).

This report does not include any representation as to the quality of HKPCA’s services beyond those covered by [WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.8](#), nor the

¹ The Hong Kong Standard on Assurance Engagement 3000 (Revised), Assurance Engagements other than Audits or Reviews of Historical Financial Information is based on the International Standard on Assurance Engagements (ISAE) 3000 (Revised), Assurance Engagements other than Audits or Reviews of Historical Financial Information of the International Auditing and Assurance Standards Board (IAASB), published by the International Federation of Accountants (IFAC) in April 2020.

suitability of any of HKPCA's services for any customer's intended purpose.

Other Matters

HKPCA's management has disclosed two incidents (see [Appendix B](#)) during the period from 1 December 2022 to 30 November 2023. 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.

Purpose and Restriction on Use

The management's assertion was prepared for obtaining and displaying the WebTrust Seal on HKPCA website² 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 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.

Use of the WebTrust seal

HKPCA's use of the WebTrust for Certification Authorities Seal constitutes a symbolic representation of the contents of the content 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, 22 February 2024

² 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.



羅兵咸永道

Appendix A – Auditor’s information

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



Appendix B – Publicly disclosed incidents

Bugzilla ID	Disclosure	Publicly Disclosed Link
1804843	Hongkong Post: Subject CN converted to Unicode representation incident	Bugzilla Ticket Link
1836694	Hongkong Post: Invalid EV cert businessCategory	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
<u>Subject DN</u> C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post Root CA 3 <u>SHA-1 Thumbprint</u> 58A2D0EC2052815BC1F3F86402244EC28E024B02 <u>SHA-256 Thumbprint</u> 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
<u>Subject DN</u> C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post e-Cert SSL CA 3 - 17 <u>SHA-1 Thumbprint</u> 92797871DC6A0B6EE1417BB657D7ED6FC6F975EB <u>SHA-256 Thumbprint</u> 69ECDBC3147F581DFDCB522D9DEFB260B26784AD4955C74E6A52522CCC4C4408		
2	Hongkong Post e-Cert EV SSL CA 3 - 17	Valid from 3 June 2017 for issuance of EV SSL certificate
<u>Subject DN</u> C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post e-Cert EV SSL CA 3 - 17 <u>SHA-1 Thumbprint</u> 6CA9BB1B3BAEF67D6D5414132A7EFB212836639E <u>SHA-256 Thumbprint</u> C18D53BF9864DD09BCBCACFD672E2566D4C81F6889E36DF5DD425C04211D0763		

3	Hongkong Post Root CA 3	Cross certificate signed by Hongkong Post Root CA 1 and revoked on 12 August 2017
<p><u>Subject DN</u> C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post Root CA 3</p> <p><u>SHA-1 Thumbprint</u> D0D535192598FCA8B68789EDCEF1EA51B3A898A5</p> <p><u>SHA-256 Thumbprint</u> ABFA404ECEEA854381ABE294AC829440E0133E077911A67E1293CF111AC43C44</p>		
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
<p><u>Subject DN</u> C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post Root CA 3</p> <p><u>SHA-1 Thumbprint</u> 97FC47E174E2AA5332321DCFF6077A19F04387F0</p> <p><u>SHA-256 Thumbprint</u> 176AEBF2972BD6F47179EDE3DE63848B1543B45AE2954BEA45185B152537B9C4</p>		
5	Hongkong Post Root CA 3	Cross certificate signed by Hongkong Post Root CA 1 and revoked on 27 July 2022
<p><u>Subject DN</u> C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post Root CA 3</p> <p><u>SHA-1 Thumbprint</u> 881700C3346CBA89A8C1C5C44A584A8441319944</p> <p><u>SHA-256 Thumbprint</u> F8F6037491861C069D3BB442B78A3DB4049EE7787B7C2841A7BA6966B5272F2C</p>		

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
<p><u>Subject DN</u> C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post Root CA 3</p> <p><u>SHA-1 Thumbprint</u> 3069BCFC8DD0AFBAABA5CA81D23CCC6413131F6F</p> <p><u>SHA-256 Thumbprint</u> 5544A24FEB21F681F1987D30E0AF5C49E9F9FFFD5550A889B40B1EC9CC81E667</p>		
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
<p><u>Subject DN</u> C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post Root CA 3</p> <p><u>SHA-1 Thumbprint</u> AF0F1F7AFBD02E3DDE39BD0B646CF97B7D122408</p> <p><u>SHA-256 Thumbprint</u> 00482341B104A0DE6E0F1D508DB84CB514F7494FE04982133A5C750136C55DC8</p>		



Appendix D - List of HKPCA's Certification Practice Statements

Document Names	Version
CPS for e-Cert (Server)	OID = 1.3.6.1.4.1.16030.1.7.16 (valid from 8 June 2023) OID = 1.3.6.1.4.1.16030.1.7.17 (valid from 1 July 2023) 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) ^

^ Latest CPS version

PricewaterhouseCoopers
22/F Prince's Building
Central
Hong Kong

22 February 2024

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 2022 to 30 November 2023

The Postmaster General operates as a Certification Authority (“CA”) known as Hongkong Post Certification Authority (“HKPCA”) through its Root CAs and Subordinate CAs referenced in Appendix A to provide its EV SSL CA Services.

The Government of the Hong Kong Special Administrative Region of the People’s Republic of China has appointed Certizen Limited (“Certizen”) as an agent of HKPCA on 24 June 2019 and 28 September 2022 for operating and maintaining the systems and services of HKPCA for the period from 1 January 2020 to 30 June 2022, and an extended period up to 30 June 2023 (date inclusive), and from 1 July 2023 to 30 June 2026 respectively. As such, HKPCA with Certizen as the agent is responsible for the management assertions of HKPCA’s operations.

HKPCA with 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, 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.

HKPCA with Certizen as its agent has assessed its disclosures of its certificate practices and controls over its EV SSL CA operations. Based on that assessment, in management’s opinion, HKPCA with Certizen as its agent, in providing its CA services in the Hong Kong Special Administrative Region, during the period from 1 December 2022 to 30 November 2023, 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 and provided such services in accordance with its CPS; and

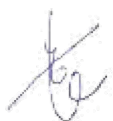
- maintained effective controls to provide reasonable assurance that:
 - the integrity of keys and EV SSL certificates it manages is established and protected throughout their lifecycles; and
 - EV SSL subscriber information is properly collected, authenticated (for the registration activities performed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

in accordance with [WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.8](#).

Yours faithfully,



(Charles 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
<u>Subject DN</u> C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post Root CA 3 <u>SHA-1 Thumbprint</u> 58A2D0EC2052815BC1F3F86402244EC28E024B02 <u>SHA-256 Thumbprint</u> 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
<u>Subject DN</u> C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post e-Cert SSL CA 3 - 17 <u>SHA-1 Thumbprint</u> 92797871DC6A0B6EE1417BB657D7ED6FC6F975EB <u>SHA-256 Thumbprint</u> 69ECDBC3147F581DFDCB522D9DEFB260B26784AD4955C74E6A52522CCC4C4408		
2	Hongkong Post e-Cert EV SSL CA 3 - 17	Valid from 3 June 2017 for issuance of EV SSL certificate
<u>Subject DN</u> C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post e-Cert EV SSL CA 3 - 17 <u>SHA-1 Thumbprint</u> 6CA9BB1B3BAEF67D6D5414132A7EFB212836639E <u>SHA-256 Thumbprint</u> C18D53BF9864DD09BCBCACFD672E2566D4C81F6889E36DF5DD425C04211D0763		

3	Hongkong Post Root CA 3	Cross certificate signed by Hongkong Post Root CA 1 and revoked on 12 August 2017
<p><u>Subject DN</u> C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post Root CA 3</p> <p><u>SHA-1 Thumbprint</u> D0D535192598FCA8B68789EDCEF1EA51B3A898A5</p> <p><u>SHA-256 Thumbprint</u> ABFA404ECEEA854381ABE294AC829440E0133E077911A67E1293CF111AC43C44</p>		
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
<p><u>Subject DN</u> C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post Root CA 3</p> <p><u>SHA-1 Thumbprint</u> 97FC47E174E2AA5332321DCFF6077A19F04387F0</p> <p><u>SHA-256 Thumbprint</u> 176AEBF2972BD6F47179EDE3DE63848B1543B45AE2954BEA45185B152537B9C4</p>		
5	Hongkong Post Root CA 3	Cross certificate signed by Hongkong Post Root CA 1 and revoked on 27 July 2022
<p><u>Subject DN</u> C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post Root CA 3</p> <p><u>SHA-1 Thumbprint</u> 881700C3346CBA89A8C1C5C44A584A8441319944</p> <p><u>SHA-256 Thumbprint</u> F8F6037491861C069D3BB442B78A3DB4049EE7787B7C2841A7BA6966B5272F2C</p>		

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
<p><u>Subject DN</u> C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post Root CA 3</p> <p><u>SHA-1 Thumbprint</u> 3069BCFC8DD0AFBAABA5CA81D23CCC6413131F6F</p> <p><u>SHA-256 Thumbprint</u> 5544A24FEB21F681F1987D30E0AF5C49E9F9FFFD5550A889B40B1EC9CC81E667</p>		
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
<p><u>Subject DN</u> C=HK, ST=Hong Kong, L=Hong Kong, O=Hongkong Post, CN=Hongkong Post Root CA 3</p> <p><u>SHA-1 Thumbprint</u> AF0F1F7AFBD02E3DDE39BD0B646CF97B7D122408</p> <p><u>SHA-256 Thumbprint</u> 00482341B104A0DE6E0F1D508DB84CB514F7494FE04982133A5C750136C55DC8</p>		

Appendix B

List of HKPCA's Certification Practice Statements

Document Names	Version
CPS for e-Cert (Server)	OID = 1.3.6.1.4.1.16030.1.7.16 (valid from 8 June 2023) OID = 1.3.6.1.4.1.16030.1.7.17 (valid from 1 July 2023) 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) ^

^ Latest CPS version