pwc 羅兵咸永道

Independent Auditor's Assurance Report
(Webtrust Principles And Criteria for Certification Authorities – Extended Validation SSL Version 1.6.2)

Independent auditor's assurance report

To Management of Hongkong Post Certification Authority:

We have been engaged to perform a reasonable assurance engagement to report on the management's assertion on extended validation SSL ("EV SSL") from 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 during the period from 1 April 2018 to 30 November 2018 for its Root CAs and Subordinate CAs referenced in Appendix A, as to whether HKPCA with Certizen as its agent has:

- prepared its EV SSL certificate lifecycle management business practices in its Certificate Practice Statements ("CPS") including its commitment to provide EV SSL certificates in conformity with the CA/Browser Forum Guidelines and to provide such services in accordance with its disclosed practices referenced in Appendix B; 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 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 Version 1.6.2.

Certification Authority's Responsibilities
HKPCA with Certizen as its agent is responsible for its 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 Version 1.6.2.

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.

Auditor's Responsibilities
It is our responsibility to express an opinion on the management's assertion based on our work performed and to report our opinion solely to you, as a body, in accordance with our agreed terms of engagement and for no other purpose. We do not assume responsibility towards or accept liability to any other person for the contents of this report.

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.

December 2018

Independent Auditor's Assurance Report
(Webtrust Principles And Criteria for Certification Authorities – Extended Validation SSL Version 1.6.2)

A reasonable assurance engagement involves performing procedures to obtain sufficient appropriate evidence whether management assertion is prepared, in all material respects, in accordance with the Webtrust Principles and Criteria for Certification Authorities – Extended Validation SSL Version 1.6.2. 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:

- obtaining an understanding of HKPCA's EV SSL key and certificate lifecycle management business practices, including its controls over the issuance, renewal, and revocation of EV SSL certificates;
- evaluating the suitability of the design of the controls; and
- 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.

For auditor's information, please refer to Appendix C.

Suitability of controls
The suitability of the design of the 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 suitability of the design of the controls at individual subscribers and relying party locations.

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, detect, or correct errors, frauds, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

Opinion
In our opinion, except for the controls documented in Appendix D that did not have any occurrences to support the operating effectiveness testing in the period from 1 April 2018 to 30 November 2018, the management's assertion, as referred to above is prepared in all material respects, in accordance with the Webtrust Principles and Criteria for Certification Authorities – Extended Validation SSL Version 1.6.2.

Purpose and Restriction on Use and Distribution
Without modifying our opinion, we draw attention to the fact that the management's assertion was prepared for the independent assessment using the Webtrust Principles and Criteria for Certification Authorities – Extended Validation SSL Version 1.6.2 designed for this purpose. As a result, the management assertion may not be suitable for another purpose.

This report does not include any representation as to the quality of HKPCA's services beyond those covered by the Webtrust Principles and Criteria for Certification Authorities – Extended Validation SSL Version 1.6.2, nor the suitability of any of HKPCA's services for any customer's intended purpose.

December 2018

羅兵咸永道

Independent Auditor's Assurance Report
(Webtrust Principles And Criteria for Certification Authorities – Extended Validation SSL Version 1.6.2)

PricewaterhouseCoopers
Certified Public Accountants

Hong Kong, 21 December 2018

Independent Auditor's Assurance Report
(Webtrust Principles And Criteria for Certification Authorities – Extended Validation SSL Version 1.6.2)

Appendix A – List of HKPCA's Root CA and Subordinate 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 58:A2:D0:EC:20:52:81:5B:C1:F3:F8:64:02:24:4E:C2:8E:02:4B:02 SHA-256 Thumbprint 5A:2F:C0:3F:0C:83:B0:90:BB:FA:40:60:4B:09:88:44:6C:76:36:18:3D:F9:84:6E:17:10:1A:44:7F:B8:EF:D6		

List of HKPCA's Subordinate CA:

Reference	Root CA Name	Remarks
1	Hongkong Post e-Cert EV SSL CA 3 – 17	Valid from 3 June 2017
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 6C:A9:BB:1B:3B:AE:F6:7D:6D:54:14:13:2A:7E:FB:21:28:36:63:9E SHA-256 Thumbprint C1:8D:53:BF:98:64:DD:09:BC:BC:AC:FD:67:2E:25:66:D4:C8:1F:68:89:E3:6D:F5:DD:42:5C:04:21:1D:07:63		

Independent Auditor's Assurance Report
(Webtrust Principles And Criteria for Certification Authorities – Extended Validation SSL Version 1.6.2)

Appendix B – List of HKPCA's Certificate Practice Statement

Document Names	Version
CPS for e-Cert (Server)	OID = 1.3.6.1.4.1.16030.1.7.4 (The service covered in this CPS had not yet been disclosed and made available to the public as at 30 November 2018. Certificates were issued for internal use on 30 May 2018 that followed change management process of HKPCA with Certizen as its agent, using HKPCA's own domain name "eCert.gov.hk", which was to serve the purpose of testing by Mozilla and its CA Community. As no EV SSL certificates were issued to external subscribers, the procedures outlined in the CPS were not fully applicable for sampling checking purpose.)

Independent Auditor's Assurance Report
(Webtrust Principles And Criteria for Certification Authorities – Extended Validation SSL Version 1.6.2)

Appendix C – Auditor's information

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

Independent Auditor's Assurance Report
(Webtrust Principles And Criteria for Certification Authorities – Extended Validation SSL Version 1.6.2)

Appendix D – Summary of Controls with No Occurrences

The followings are the controls set out in the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL Version 1.6.2 that did not have any occurrences at HKPCA with Certizen as its agent to support the operating effectiveness testing in the period from 1 April 2018 to 30 November 2018, due to the fact that only EV SSL certificates were issued for internal use within HKPCA which followed change management process of HKPCA with Certizn as its agent, and no EV SSL certificates were issued to any external subscribers during the period from 1 April 2018 to 30 November 2018.

a) Application enrolment process;
b) Verification of new application to ensure the validity of the subscribers according to application requirement;
c) Identification and authentication of new application;
d) Information included in the Certificate Revocation List;
e) Timely Update of Certificate Revocation List to ensure the CRLs are updated to the website on a daily basis;
f) Verification of renewal request;
g) Identification and authentication of renewal request;
h) Revokation process to ensure the completeness of revocation procedure according to receipt date & time;
i) Retention of all documentation relating to certificate requests (i.e., related to application for EV SSL certificates) and the verification thereof, and all Certificates and revocation thereof; and
j) Retention of audit logs (i.e., related to application for EV SSL certificates) to ensure the completeness of daily log review, verification of daily backup tapes, checking of alerts and abnormalities, and authorization.

PricewaterhouseCoopers
22/F Prince's Building
Central
Hong Kong

21 December 2018

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 April 2018 through 30 November 2018

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 has appointed Certizen Limited ("Certizen") as an agent of HKPCA on 13 October 2011 for operating and maintaining the systems and services of HKPCA from 1 April 2012 to 31 March 2018, which has been subsequently extended to 31 December 2019. 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 of the People's Republic of China, during the period from 1 April 2018 through 30 November 2018, HKPCA with Certizen as its agent has:

- disclosed its EV SSL certificate lifecycle management business practices in its Certificate Practice Statements ("CPS") that published on 21 December 2018 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;
- 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 version 1.6.2.

Yours faithfully,

(Leonard LAM)
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 58:A2:D0:EC:20:52:81:5B:C1:F3:F8:64:02:24:4E:C2:8E:02:4B:02 SHA-256 Thumbprint 5A:2F:C0:3F:0C:83:B0:90:BB:FA:40:60:4B:09:88:44:6C:76:36:18:3D:F9:84:6E:17:10:1A:44:7F:B8:EF:D6		

List of HKPCA's Subordinate CA:

Reference	Root CA Name	Remarks
1	Hongkong Post e-Cert EV SSL CA 3 – 17	Valid from 3 June 2017
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 6C:A9:BB:1B:3B:AE:F6:7D:6D:54:14:13:2A:7E:FB:21:28:36:63:9E SHA-256 Thumbprint C1:8D:53:BF:98:64:DD:09:BC:BC:AC:FD:67:2E:25:66:D4:C8:1F:68:89:E3:6D:F5:DD:42:5C:04:21:1D:07:63		

Appendix B

List of HKPCA's Certificate Practice Statement

Document Names	Version
CPS for e-Cert (Server)	OID = 1.3.6.1.4.1.16030.1.7.4 (The service covered in this CPS had not yet been disclosed and made available to the public as at 30 November 2018. Certificates were issued for internal use on 30 May 2018 that followed change management process of HKPCA with Certizen as its agent, using HKPCA's own domain name "eCert.gov.hk", which was to serve the purpose of testing by Mozilla and its CA Community. As no EV SSL certificates were issued to external subscribers, the procedures outlined in the CPS were not fully applicable for sampling checking purpose.)