Ernst & Young
62/F One Island East
18 Westlands Road
Island East
Hong Kong

安永會計師事務所
香港港島東華蘭路 18 號
港島東中心 62 樓

Tel 電話: +852 2846 9888
Fax 傳真: +852 2868 4432
ey.com

31 March, 2016

Report of Independent Accountants

To the Management of Hongkong Post Certification Authority:

We have examined the assertion by the management of the Hongkong Post Certification Authority ("HKPCA"), with Certizen Limited ("Certizen") as an agent of HKPCA[1], regarding the disclosure of its key and SSL certificate life cycle management business practices and procedures and the effectiveness of its controls over the authenticity of subscriber information, key and SSL certificate integrity, logical and physical access to HKPCA's Certification Authority ("CA") systems and data, the continuity of key and certificate management operations, development, maintenance and operation of CA systems integrity and the Network and Certificate system Security Requirements set forth by the CA/Browser Forum, based on the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.0 ("SSL Baseline Requirements") for its SSL Certification Authority ("CA") service through its Root CA and Subordinate CA referenced in Appendix A, in the Hong Kong Special Administrative Region of the People's Republic of China, during the period 1 September, 2015 through 31 December, 2015.

HKPCA with Certizen as its agent is responsible for the management assertions. Our responsibility is to express an opinion on management's assertion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included (1) obtaining an understanding of HKPCA's key and SSL certificate life cycle management business practices and its controls over key and SSL certificate integrity, over the continuity of key and SSL certificate life cycle management operations, and over the development, maintenance and operation of systems' integrity; (2) selectively testing transactions executed in accordance with disclosed key and SSL certificate life cycle 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. We believe that our examination provides a reasonable basis for our opinion.

In performing our examination, we noted that SSL subscriber certificates issued by the HKPCA's Subordinate CA - "Hongkong Post e-Cert CA 1 – 10" and "Hongkong Post e-Cert CA 1 – 14", during the period from 1 September, 2015 through 31 December, 2015, did not meet with the Certificate Content and profile requirements as set out in CA/Browser Forum Baseline Requirements - Section 9 and appendix B and therefore prevented Principle 2, Criterion 2.1, 2.2 and 2.3 of the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.0 from being met.

[1] HKPCA operations have been outsourced to Certizen for operating and maintaining the systems and services of HKPCA from 1 April 2012 to 31 March 2018, as disclosed in HKPCA's business practices disclosure.

We were represented by the management of the HKPCA with the business needs to support and maintain aforementioned SSL subscriber certificates for its applicants. We further noted from the management of the HKPCA and relevant publicly disclosed information, HKPCA has established transition plans to stop issuing SSL subscriber certificates under the Subordinate CA - "Hongkong Post e-Cert CA 1 – 10" from 1 January, 2016 and SSL subscriber certificates under the Subordinate CA - "Hongkong Post e-Cert CA 1 – 14" from 1 September, 2016.

In our opinion, except for the effects of the matter(s) discussed in the preceding paragraph, in providing its SSL CA services in the Hong Kong Special Administrative Region of the People's Republic of China through its Root CA and Subordinate CA referenced in Appendix A, during the period 1 September, 2015 through 31 December, 2015, HKPCA has, in all material respects:

- Disclosed its certificate practices and procedures and its commitment to provide SSL Certificates in conformity with the applicable CA/Browser Forum Guidelines.
- Maintained effective controls to provide reasonable assurance that:
    - Subscriber information was properly collected, authenticated (for the registration activities performed by HKPCA) and verified; and
    - The integrity of keys and certificates it manages was established and protected throughout their life cycles.
- Maintained effective controls to provide reasonable assurance that:
    - Logical and physical access to CA systems and data was restricted to authorized individuals;
    - The continuity of key and certificate management operations was maintained;
    - CA system development, maintenance and operations were properly authorized and performed to maintain CA systems' integrity; and
    - Met the Network and Certificate system Security Requirements set forth by the CA/Browser Forum.

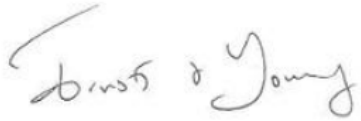
based on the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.0.

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.

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 conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

This report does not include any representation as to the quality of HKPCA's certificate services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.0, nor the suitability of any of HKPCA's services for any customer's intended purpose.

Yours faithfully,



31 March, 2016

Assertion by Management Regarding the Disclosure of the Certificate Practices and the Controls Over the Hongkong Post Certification Authority SSL Certification Authority Services During the Period 1 September 2015 through 31 December 2015

Hongkong Post Certification Authority ("HKPCA") provides SSL Certification Authority ("CA") services in the Hong Kong Special Administrative Region of the People's Republic of China through the Root CA and Subordinate CA referenced in Appendix A.

The HKPCA operations were outsourced to Certizen Limited ("Certizen") on 13 October 2011 for operating and maintaining the systems and services of HKPCA from 1 April 2012 to 31 March 2018, as disclosed in HKPCA's business practices disclosures. HKPCA with Certizen as its agent is responsible for the management assertions of the HKPCA operations.

HKPCA with Certizen as its agent, has assessed the disclosure of its Certificate practices and procedures and its controls over its SSL Certification Authority ("CA") services in the Hong Kong Special Administrative Region of the People's Republic of China through the Root CA and Subordinate CA referenced in Appendix A for the period 1 September 2015 to 31 December 2015. Based on that assessment, in management's opinion, in providing its SSL CA services in the Hong Kong Special Administrative Region of the People's Republic of China, during the period 1 September 2015 through 31 December 2015, HKPCA has:

- Disclosed its Certificate practices and procedures and its commitment to provide SSL Certificates in conformity with the applicable CA/Browser Forum Guidelines.

- Maintained effective controls to provide reasonable assurance that:
  - Subscriber information was properly collected, authenticated (for the registration activities performed by HKPCA with Certizen as its agent) and verified; and
  - The integrity of keys and certificates it managed was established and protected throughout their life cycles.

- Maintained effective controls to provide reasonable assurance that:
  - Logical and physical access to CA systems and data was restricted to authorized individuals;
  - The continuity of key and certificate management operations was maintained;
  - CA system development, maintenance and operations were properly authorized and performed to maintain CA systems' integrity; and
  - Met the Network and Certificate system Security Requirements set forth by the CA/Browser Forum.

based on the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.0, except for the effects of the matter in the following paragraphs:

Principle 2, Criterion 2.1, 2.2 and 2.3 of the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.0 requires that, with respect to

certificates issued, the CA maintains controls to provide reasonable assurance that the certificates issued meet the minimum requirements for Certificate Content and profile as established in Section 9 of CA/Browser Forum SSL Baseline Requirements including Section 9.1 to 9.7, appendix A and appendix B.

The SSL subscriber certificates issued by the HKPCA's Subordinate CA - "Hongkong Post e-Cert CA 1 – 10" and "Hongkong Post e-Cert CA 1 – 14", during the period from 1 September 2015 through 31 December 2015, did not meet with the Certificate Content and profile requirements as set out in CA/Browser Forum Baseline Requirements - Section 9 and appendix B.

The management has asserted the business needs to support and maintain aforementioned SSL subscriber certificates for its applicants. The management has established and publicly disclosed its transition plans to stop issuing SSL subscriber certificates under the Subordinate CA - "Hongkong Post e-Cert CA 1 – 10" from 1 January 2016 and SSL subscriber certificates under the Subordinate CA "Hongkong Post e-Cert CA 1 – 14" from 1 September 2016.

Yours faithfully

(Leonard LAM)
for Postmaster General

(Eva CHAN)
for Certizen Limited

Appendix A

List of HKPCA's Root CA:

Reference	Root CA Name
1	Hongkong Post Root CA 1
2	Hongkong Post Root CA 2

List of HKPCA's Subordinate CA:

Reference	Subordinate CA Name
1	Hongkong Post e-Cert CA 1 - 10
2	Hongkong Post e-Cert CA 1 - 14
3	Hongkong Post e-Cert CA 1 - 15
4	Hongkong Post e-Cert CA 2 - 15