INDEPENDENT PRACTITIONER'S ASSURANCE REPORT

To the Management of China Financial Certification Authority Co., Ltd

We have been engaged to perform a reasonable assurance engagement on the accompanying assertion of China Financial Certification Authority Co., Ltd ("CFCA") for its SSL Certification Authority operations for the period from August 1st, 2018 to July 31st, 2019.

Management's Responsibilities

CFCA's management 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 – SSL Baseline with Network Security Version 2.4.1.

Our Independence and Quality Control

We have complied with the independence and other ethical requirement of the Code of Ethics for Professional Accountants 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 Control 1 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 accompanying assertion of CFCA based on our work performed.

We conducted our work in accordance with the International Standard on Assurance Engagements 3000 (Revised) "Assurance Engagements Other Than Audits or Reviews of Historical Financial Information". This standard requires that we plan and perform our work to form the opinion.

INDEPENDENT PRACTITIONER'S ASSURANCE REPORT (Continued)

A reasonable assurance engagement involves performing procedures to obtain sufficient appropriate evidence whether the management's assertion of CFCA is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security Version 2.4.1. 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 CFCA's SSL certificate life cycle management business practices, including its relevant controls over the issuance, renewal and revocation of SSL certificates, and obtaining an understanding of CFCA's network and certificate system security to meet the requirements set forth by the CA/Browser Forum;
(2) selectively testing transactions executed in accordance with disclosed SSL certificate lifecycle management 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 the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

The relative effectiveness and significance of specific controls at CFCA 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 do not provide any assurance on the effectiveness of controls at individual subscribers and relying party locations.

Inherent Limitation

We draw attention to the fact that the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security Version 2.4.1 includes certain inherent limitations that can influence the reliability of the information.

Because of the nature and inherent limitations of controls, CFCA'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.

INDEPENDENT PRACTITIONER'S ASSURANCE REPORT (Continued)

Opinion

In our opinion, the accompanying assertion of CFCA, for the period from August 1st, 2018 to July 31st, 2019, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security Version 2.4.1.

Emphasis of Matters

Without modifying our conclusion, we draw attention to the below matters:

1) The cryptographic device being used to generate keys was manufactured by its vendor to meet the mandatory standards and requirements set out by the Office of State Commercial Cryptography Administration (OSCCA) in China. The vendor represented to CFCA that the cryptographic device being used by CFCA has been designed to fulfill the physical security and management control aspects of the FIPS140-2 Level 3 standard.

2) This report does not include any representation as to the quality of CFCA's certification services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security Version 2.4.1, nor the suitability of any of CFCA's services for any customer's intended purpose.

Other Matters

The WebTrust Seal of assurance for Certification Authorities on CFCA's Website 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.

INDEPENDENT PRACTITIONER'S ASSURANCE REPORT (Continued)

Purpose and Restriction on Use and Distribution

Without modifying our opinion, we draw attention to the fact that the accompanying assertion of CFCA was prepared for obtaining and displaying the WebTrust Seal[1] on its website using the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security Version 2.4.1 designed for this purpose. As a result, the accompanying assertion of CFCA may not be suitable for another purpose. This report is intended solely for the Management of CFCA in connection with obtaining and displaying the WebTrust Seal on its website after submitting the report to the related authority in connection with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security Version 2.4.1 and should not be distributed to or used by any other parties for any other purpose. We do not assume responsibility towards or accept liability to any other person for the contents of this report.

PricewaterhouseCoopers Zhong Tian LLP

PRICEWATERHOUSECOOPERS ZHONG TIAN LLP BEIJING BRANCH
普华永道中天会计师事务所(特殊普通合伙)北京分所
11010300479884

PricewaterhouseCoopers Zhong Tian LLP Beijing Branch
Beijing, China
October 31, 2019

[1] *The maintenance and integrity of the CFCA website is the responsibility of the directors; 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 assertion by the management of CFCA on which the assurance report was issued or the assurance report that was issued and the information presented on the website.*

China Financial Certification Authority Co.,Ltd
20-3 Pingyuanli, Caishikou South Avenue
Xi Cheng District, Beijing , PRC
Tel:010-83526355
Fax:010-63555032
Http://www.cfca.com.cn

PricewaterhouseCoopers ZhongTian LLP, Beijing Branch
26/F Tower A
Beijing Fortune Plaza, 7 DongsanhuanZhong Road
Chaoyang District, Beijing 100020, PRC

October 31, 2019

Dear Members of the Firm,

Assertion by Management of China Financial Certification Authority Co,.Ltd. regarding its Disclosure of its Certificate Practices and its Controls Over its SSL Certification Authority Services during the period from August 1, 2018 through July 31 ,2019

China Financial Certification Authority Co,. Ltd. ("CFCA") operates the Certification Authority (CA) services known as a root CA in scope for SSL Baseline Requirements and Network Security Requirements and provides SSL CA services.

CFCA management has assessed its disclosures of its certificate practices and controls over its EV SSL CA services. Based on that assessment, in providing its SSL Certification Authority (CA) services at Beijing, China, throughout the period August 1, 2018 to July 31, 2019, CFCA has:

- disclosed its SSL certificate lifecycle management business practices in its:
  - Certification Practice Statement Of CFCA Global-Trust System v4.0 (http://www.cfca.com.cn/upload/CertificationPracticeStatementOfCFCAGlobal-TrustSystemCHN.pdf), and
  - Certificate Policy Of CFCA v 3.0 (http://www.cfca.com.cn/upload/CertificatePolicyOfCFCA.pdf)

  including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the CFCA website, and provided such services in accordance with its disclosed practices.

- maintained effective controls to provide reasonable assurance that:
  - The integrity of keys and SSL certificates it manages is established and protected throughout their lifecycles; and
  - SSL subscriber information is properly authenticated (for the registration activities performed by CFCA)
- 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;
- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security Version 2.4.1 (https://www.cpacanada.ca/-/media/site/operational/ms-member-services/docs/webtrust/wtbr-241-final--ssl-baseline-with-network-security-june-30-2019.pdf?la=en&hash=4F84AA9365F7B8E2AFE5AD2A5FC6579D94CA6D2D).

[CFCA Representative]

中金金融认证中心有限公司

[Title of the representative]

Appendix

The List of keys and certificates covered in the management assessment is as follow:

CA #	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
1	1	CN = CFCA EV ROOT O = China Financial Certification Authority C = CN	CN = CFCA EV ROOT O = China Financial Certification Authority C = CN	18 4a cc d6	rsaEncryption	4096 bits	sha256WithRSAEncryption	August 08, 2012	December 31, 2029	e3 fe 2d fd 28 d0 0b b5 ba b6 a2 c4 bf 06 aa 05 8c 93 fb 2f	5C:C3:D7:8E:4E:1D:5E:45:54:7A:04:E6:87:3E:64:F9:0C:F9:53:6D:1C:CC:2E:F8:00:F3:55:C4:C5:FD:70:FD
2	1	CN = CFCA EV OCA O = China Financial Certification Authority C = CN	CN = CFCA EV ROOT O = China Financial Certification Authority C = CN	00 b4 cf 94 32 66	rsaEncryption	2048 bits	sha256WithRSAEncryption	August 08, 2012	December 29, 2029	55 08 e2 dc cc 95 6d 1f 5d de b3 47 e8 e9 16 c6 c0 45 77 c4	CC:72:53:EB:DE:9F:7E:92:CB:A2:97:B5:BA:DE:D1:B2:2E:5C:EA:CA:52:5E:20:1B:4D:C4:10:F4:F3:50:4B:5E
3	1	CN = CFCA OV OCA O = China Financial Certification Authority C = CN	CN = CFCA EV ROOT O = China Financial Certification Authority C = CN	00 f9 df 6a df f5 64 be a6 8b 82	rsaEncryption	2048 bits	sha256WithRSAEncryption	March 25, 2015	December 25, 2029	66 b3 ef fb 54 95 87 e9 ac a5 96 56 ae e6 7d ed 3a d0 43 d1	F0:7B:BB:DE:07:6F:9B:40:C5:7C:C4:BE:FE:DE:97:CA:1F:53:B9:AE:14:7F:03:5D:28:4C:BF:53:F3:43:2F:B8