pwc

普华永道

INDEPENDENT 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 by the management of China Financial Certification Authority Co., Ltd ("CFCA") for its SSL Certification Authority operations during the period from March 16th, 2014 to September 30th, 2014.

Management's Responsibility for the management's assertion of CFCA Certification Authority

CFCA Certification Authority has suitably designed its practices and procedures based on AICPA/CPA Canada WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security Version 2.0. CFCA's management is responsible for the preparation and presentation of the management's assertion in accordance with the AICPA/CPA Canada WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security Version 2.0. This responsibility includes designing, implementing and maintaining the internal control relevant to the preparation and presentation of the management's assertion of CFCA Certification Authority, applying an appropriate basis of preparation, and making estimates that are reasonable in the circumstances.

Auditor's Responsibility

It is our responsibility, to express a conclusion on the management's assertion of CFCA Certification Authority based on our work performed and to report our conclusion solely to you, as a body, in accordance with our agreed terms of engagement, for management to submit to the related authority to obtain and display the WebTrust Seal[1] on its website, 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 the International Standard on Assurance Engagements 3000 "Assurance Engagements Other Than Audits or Reviews of Historical Financial Information". This standard requires that we comply with ethical requirements and plan and perform the assurance engagement to obtain reasonable assurance over whether the management's assertion of CFCA Certification Authority complies in all material respects with the AICPA/CPA Canada WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security Version 2.0.

---

[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.*

A reasonable assurance engagement involves performing procedures to obtain sufficient appropriate evidence over whether the management's assertion of CFCA Certification Authority complies in all material respects with the AICPA/CPA Canada WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security Version 2.0. The procedures selected depend on the auditor's judgment, including the assessment of the risks of material non-compliance with the management's assertion of CFCA Certification Authority with the AICPA/CPA Canada WebTrust.

Principles and Criteria for Certification Authorities – SSL Baseline with Network Security Version 2.0. 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 practices and procedures, including its relevant controls over the issuance, renewal and revocation of SSL certificates, (2) evaluating whether the design of practices and procedures complies with the AICPA/CPA Canada WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security Version 2.0, (3) testing and evaluating the operating effectiveness of the control, 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 conclusion.

Inherent Limitation

We draw attention to the fact that the AICPA/CPA Canada WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security Version 2.0 includes certain inherent limitations that can influence the reliability of the information.

Because of inherent limitations in controls, error, fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements may not be prevented, corrected or detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that (1) changes made to the system or controls, (2) changes in processing requirements, (3) changes required because of the passage of time, or (4) degree of compliance with the policies or procedures may alter the validity of such conclusions.

Conclusion

In our opinion, the accompanying assertion by the management of CFCA, for the period from March 16th, 2014 to September 30th, 2014, complies in all material respects with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security Version 2.0.

Emphasis of Matters

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

1) The cryptographic device being used to generate keys was manufactured by its vendor supplier to meet the mandatory standards and requirements set out by Office of State Commercial Cryptography Administration (OSCCA) in China. The vendor supplier 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) 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.

3) 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 2.0, or the suitability of any of CFCA's services for any customer's intended purpose.

4) 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.

Our conclusion is not modified in respect of the above matters.

Restriction on Use and Distribution

Our report is intended solely for CFCA to obtain and display 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 2.0 and may not be suitable for another purpose. This report is not intended to be, and should not be distributed to or used, for any other purpose.

PricewaterhouseCoopers Zhong Tian LLP Beijing Branch

December 5th, 2014

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 DongsuanhuanZhong Road
Chaoyang District, Beijing 100020, PRC

September 30, 2014

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 Overits SSL Certification Authority Services during the periodfrom March 16th, 2014 through September 30th ,2014.

The management of China Financial Certification Authority Co,. Ltd.(CFCA) has assessed the disclosure of itscertificate practices and its controls over its CA - SSL services located at Mainland China, during the period from March 16th, 2014 through September 30th,2014.The keysand certificates covered in our assessment are listed in the **Appendix** of this letter. Based on that assessment, in CFCAManagement's opinion, inproviding its CA - SSL services at Mainland China, CFCA, during the period from March 16th, 2014 through September 30th,2014.,CFCA:

- Disclosed its Certificate practices and procedures and its commitment to provide SSL Certificates inconformity with the applicable CA/Browser Forum Guidelines.
- Maintained effective controls to provide reasonable assurance that:
    - The Certificate Policy and/or Certificate Practice Statement are available on a 24x7 basis and updated annually;
    - Subscriber information was properly collected, authenticated (for the registration activitiesperformed by the CA) and verified;
    - The integrity of keys and certificates it manages was established and protected throughouttheir life cycles;
    - 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 systems development, maintenance and operations were properly authorized andperformed to maintain CA systems integrity; and
    - CA's network and certificate system security were properly managed.

in accordance with the WebTrust® Principles and Criteria for Certification Authorities – SSL Baseline with Network Security Version 2.0.

Miss JiXiaojie
General Manager of China Financial Certification AuthorityCo.,Ltd

Appendix:

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

Key name	Key type	Key size	Algorithm	Certificates (thumbprint)	Certificates Signed by The key
CFCA EV ROOT	Root key	RSA 4096 bits	SHA-256	e2 b8 29 4b 55 84 ab 6b 58 c2 90 46 6c ac 3f b8 39 8f 84 83	CFCA EV ROOT
CFCA EV OCA	Signing key	RSA 2048 bits	SHA-256	ee 41 f7 72 ab cd c9 9a 0a 3c 44 28 1d 84 06 d8 0d 29 34 2a	CFCA EV ROOT