



INDEPENDENT PRACTITIONER'S ASSURANCE REPORT

2016/BJ-181

(Page 1 of 4)

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 Certification Authority - Extended Validation SSL operations for the period from August 1st, 2015 to July 31st, 2016.

Management's Responsibility

Pursuant to regulatory requirements, CFCA's management is responsible for the preparation of the management's assertion in accordance with the CPA Canada WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL Version 1.4.5. This responsibility includes designing, implementing and maintaining the internal control relevant to the preparation of the management's assertion of CFCA, applying an appropriate basis of preparation, and making estimates that are reasonable in the circumstances.

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 Responsibility

It is our responsibility, pursuant to regulatory requirements, 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 complies in all material respects with the CPA Canada WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL Version 1.4.5. 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 EV certificate life cycle management practices and procedures, including its relevant controls over the issuance, renewal and revocation of EV certificates, (2) evaluating whether the design of practices and procedures complies with the CPA Canada WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL Version 1.4.5, (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 opinion.

Inherent Limitation

We draw attention to the fact that the CPA Canada WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL Version 1.4.5 includes certain inherent limitations that can influence the reliability of the information.

Opinion

In our opinion, the accompanying assertion of CFCA, for the period from August 1st, 2015 to July 31st, 2016, complies in all material respects with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL Version 1.4.5.



INDEPENDENT PRACTITIONER'S ASSURANCE REPORT (Continued)

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) The WebTrust EV 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 – Extended Validation SSL Version 1.4.5, 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.



普华永道

2016/BJ-181

(Page 4 of 4)

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 EV Seal¹ on its website using the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL Version 1.4.5 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 EV Seal on its website after submitting the report to the related authority in connection with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL Version 1.4.5 and should not be distributed to or used by any other person for any other purpose. We do not assume responsibility towards or accept liability to any other parties for the contents of this report.


PricewaterhouseCoopers Zhong Tian LLP Beijing Branch
Beijing, China
December 24, 2016



¹The 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.



注册会计师独立鉴证报告

2016/BJ-181

(第1页/共3页)

(注意: 本中文报告只作参考。正文请参阅英文报告。)

致: 中金金融认证中心有限公司管理层

我们接受委托, 对后附的中金金融认证中心有限公司(China Financial Certification Authority Co., Ltd, 简称“CFCA”)自2015年8月1日到2016年7月31日期间的电子认证-服务器证书增强验证证书运营的管理层认定执行了合理保证的鉴证业务。

管理层的责任

根据法规的规定, 按照CPA Canada WebTrust电子认证-服务器证书增强验证证书审计标准1.4.5版本编制和列报电子认证-服务器证书增强验证证书服务的管理层认定是CFCA管理层的责任。这种责任包括设计、执行和维护与编制和列报电子认证-服务器证书增强验证证书服务管理层认定有关的内部控制、采用适当的编制基础、以及根据情况做出合理估计。

我们的独立性与质量控制

我们遵守了国际会计师职业道德准则理事会颁布的执业会计师道德守则中的独立性及其他职业道德要求。该职业道德守则以诚信、客观、专业胜任能力及应有的关注、保密和良好职业行为为基本原则。

本事务所遵循国际质量控制准则第1号, 据此维护全面系统的质量控制体系, 包括与遵守职业道德要求、专业标准和适用的法律和法规要求相关的书面政策与程序。

注册会计师的责任

根据法规的规定, 我们的责任是在执行鉴证工作的基础上对CFCA电子认证-服务器证书增强验证证书服务的管理层认定发表意见。

我们根据《国际鉴证业务准则第3000号(修订版)--历史财务信息审计或审阅以外的鉴证业务》的规定执行了鉴证工作。该准则要求我们计划和实施鉴证工作, 以形成鉴证意见。

合理保证的鉴证业务涉及实施鉴证程序, 以获取有关CFCA电子认证服务的管理层认定是否在所有重大方面符合CPA Canada WebTrust电子认证-服务器证书增强验证证书审计标准1.4.5版本的充分、适当的证据。选择的鉴证程序取决于注册会计师的判断及我们对项目风险的评估。在我们的工作范围内, 我们实施了包括: (1)了解CFCA的增强验证电子证书生命周期管理, 包括增强验证电子证书发放、更新和吊销等相关控制; (2)评估操作规范和业务流程的设计是否符合CPA Canada WebTrust电子认证-服务器证书增强验证证书审计标准1.4.5版本; (3)测试并评估控制的有效性; 和(4)执行其他我们认为必要的鉴证程序。

我们相信, 我们获取的证据是充分、适当的, 为发表鉴证意见提供了基础。



注册会计师独立鉴证报告 (续)

固有限制

我们提请使用者注意，CPA Canada WebTrust电子认证-服务器证书增强验证证书审计标准1.4.5版本具有某些可能影响鉴证对象信息可靠性的固有限制。

意见

我们认为，CFCA自2015年8月1日至2016年7月31日期间的电子认证-服务器证书增强验证证书服务的管理层认定在所有重大方面符合CPA Canada WebTrust电子认证-服务器证书增强验证证书审计标准1.4.5版本。

强调事项

在不影响我们结论的前提下，我们提请注意如下事项：

- 1) CFCA用于产生密钥的加密设备是由一家加密设备生产商所提供。根据该加密设备生产商向CFCA的声明，CFCA所使用的加密设备符合中国国家商用密码管理办公室 (The Office of State Commercial Cryptography Administration, 简称“OSCCA”) 的有关标准及要求，并符合FIPS140-2 Level 3 在物理安全和管理的控制要求。
- 2) CFCA网站上的WebTrust增强验证电子认证标识 (“WebTrust EV Seal”) 是本报告内容的一种符号表示，它并不是为了也不应被认为是对本报告的更新或任何进一步的保证。
- 3) 本报告并不包括任何在WebTrust电子认证-服务器证书增强验证证书审计标准1.4.5版本以外的质量标准声明，或任何客户对CFCA服务的合适性声明。
- 4) CFCA的内部控制的有效性和重要性，及其对用户及相关依赖方的控制风险评估所产生的影响，取决于控制间的相互作用以及其他存在于每个用户和相关依赖方的因素。我们并没有对用户和依赖方所负责的控制的有效性进行任何评估工作。

我们的结论不因上述事项而修改。



普华永道

2016/BJ-181

(第3页/共3页)

注册会计师独立鉴证报告（续）

目的及使用和分发限制

我们提醒使用者关注，该CFCA电子认证-服务器证书增强验证证书运营的管理层认定为获得WebTrust增强验证电子认证标识¹而向有关机构提交，并采用为该目的而设计的WebTrust电子认证-服务器证书增强验证证书审计标准1.4.5版本，因此CFCA电子认证-服务器证书增强验证证书运营的管理层认定可能不适用于其他目的。本报告仅向CFCA管理层出具，用作根据WebTrust电子认证-服务器证书增强验证证书审计标准1.4.5版本的要求，为获得WebTrust增强验证电子认证标识而向有关机构提交。除了将本报告副本提供给WebTrust以外，不应向任何其他方分发或为其他目的使用。我们不会就本报告的内容向任何其他人负上或承担任何责任。本段内容不影响已发表的鉴证意见。

普华永道中天会计师事务所（特殊普通合伙）

普华永道中天会计师事务所（特殊普通合伙）北京分所

中国北京市

2016年12月24日

¹ CFCA 网站维护和网站的真实完整是公司董事的职责。我们执行的鉴证程序不包含对该等事项的考虑，因此，对出具本鉴证报告所依赖的CFCA管理层认定或鉴证报告与网站所显示信息的任何差异我们均不承担责任。

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

July 31, 2016

Dear Members of the Firm,

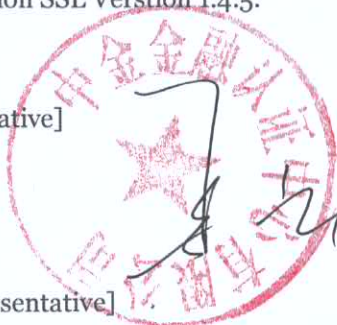
**Assertion by Management of China Financial Certification Authority Co.,Ltd.
regarding its Disclosure of its Certificate Practices and its Controls Over its
Extended Validation SSL Operations during the period from August 1, 2015
through July 31 ,2016.**

The management of China Financial Certification Authority Co., Ltd. (CFCA) has assessed the disclosure of its certificate practices and its controls over its CA - EV SSL services located at Mainland China, during the period from August 1, 2015 through July 31, 2016. The keys and certificates covered in our assessment are listed in the **Appendix** of this letter. Based on that assessment, in CFCA Management's opinion, in providing its CA - EV services at Mainland China, CFCA, during the period from August 1, 2015 through July 31, 2016, CFCA:

- Disclosed its EV Certificate practices and procedures and its commitment to provide EV SSL Certificates in conformity 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;
 - EV Subscriber information was properly collected, authenticated (for the registration activities performed by the CA) and verified;
 - The integrity of keys and EV SSL certificates it manages was established and protected throughout their life cycles;

in accordance with the WebTrust® Principles and Criteria for Certification Authorities –
Extended Validation SSL Version 1.4.5.

[CFCA Representative]



[Title of the representative]

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

中金金融认证中心有限公司
北京市西城区菜市口南大街平原里20-3
电话: 010-83526655
传真: 010-63555032
<http://www.cfca.com.cn>

普华永道中天会计师事务所（特殊普通合伙）北京分所
中国北京市朝阳区东三环中路7号
北京财富中心写字楼A座26楼

2016年7月31日

致：普华永道中天会计师事务所职业会计师：


中金金融认证中心有限公司管理层就**2015年8月1日至2016年7月31日**，对电子认证—增强验证服务器证书业务规则披露和电子认证运行控制活动的管理层认定报告（本中文报告只作参考，正文请参阅英文报告。）

中金金融认证中心有限公司（CFCA）管理层就在中国大陆提供的WebTrust电子认证—EV SSL证书服务控制已进行了评估。附件列示了评估所包括的密钥和证书。根据评估，CFCA管理层认为，就2015年8月1日至2016年7月31日CFCA提供的WebTrust电子认证—CA增强验证服务器证书服务，CFCA：

- 已披露 WebTrust 电子认证—EV SSL 证书的业务实践和程序，包含承诺遵循 CAB 论坛的相关指引提供 SSL 证书服务，并依据披露的业务实践提供相关服务；
- 通过有效控制机制，以提供以下合理保证：
 - 电子认证业务规则可 24x7 访问，并且每年更新；
 - 恰当的收集、鉴定（对 CA 内部注册机构）和验证 SSL 证书申请者的信息；
 - 有效维护密钥与EV SSL证书在生命周期中的完整性；

以符合 AICPA/CPA Canada WebTrust 电子认证—增强验证服务器证书审计标准 1.4.5。

[CFCA公司代表]
CFCA 公司代表职位



附件:

下表列示本声明所包含的密钥和证书

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