



INDEPENDENT ASSURANCE REPORT

2015/BJ-117/ATL/RYE

(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 by the management of China Financial Certification Authority Co., Ltd (“CFCA”) for its SSL Certification Authority operations during the period from October 1st, 2014 to July 31st, 2015.

Management’s Responsibility for the management’s assertion of CFCA

CFCA has suitably designed its practices and procedures based on 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 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, 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 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 Seal¹ 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

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.



INDEPENDENT ASSURANCE REPORT (Continued)

engagement to obtain reasonable assurance over whether the management's assertion of CFCA complies in all material respects with the CPA Canada WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security Version 2.0.

A reasonable assurance engagement involves performing procedures to obtain sufficient appropriate evidence over whether the management's assertion of CFCA complies in all material respects with the 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 with the 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 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 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.



INDEPENDENT ASSURANCE REPORT (Continued)

Conclusion

In our opinion, the accompanying assertion by the management of CFCA, for the period from October 1st, 2014 to July 31st, 2015, 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.



普华永道

2015/BJ-117/ATL/RYE

(Page 4 of 4)

INDEPENDENT ASSURANCE REPORT (Continued)

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
Beijing, the People's Republic of China
October 16, 2015



独立鉴证报告

2015/BJ-117/ATL/RYE

(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2014年10月1日至2015年7月31日止期间的电子认证-SSL证书运营的管理层认定执行了合理保证的鉴证业务。

管理层对电子认证—SSL证书服务管理层认定的责任

中金金融认证中心管理层已经按照CPA Canada WebTrust电子认证-SSL证书基准审计标准与网络安全2.0版本(“WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security Version 2.0”)的规定设计了操作规范和业务流程。按照CPA Canada WebTrust电子认证-SSL证书基准审计标准与网络安全2.0版本编制和列报电子认证-SSL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-SSL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。

审计师的责任

我们的职责是在执行鉴证工作的基础上对CFCA电子认证-SSL证书服务的管理层认定发表结论, 并按照双方同意的业务约定条款, 仅对贵公司报告我们的结论, 供贵公司获得WebTrust标识²(“WebTrust Seal”)而向有关机构提交, 除此之外并无其他目的。我们不会就本报告的内容向任何其他方承担责任和义务。

我们根据国际鉴证业务准则第3000号“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。该准则要求我们遵守职业道德规范, 计划和实施鉴证工作以对CFCA电子认证-SSL证书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-SSL证书基准审计标准与网络安全2.0版本获取合理保证。

合理保证的鉴证工作包括实施鉴证程序, 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-SSL证书基准审计标准与网络安全2.0版本的充分适当的证据。选择的鉴证程序取决于审计师的判断, 包括对CFCA电子认证服务的管理层认定存在重大不符合CPA Canada WebTrust电子认证-SSL证书基准审计标准与网络安全2.0版本风险的评估。在我们的鉴证工作范围内, 我们实施了包括: (1)了解CFCA的SSL电子证书生命周期管理, 包括SSL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-SSL证书基准审计标准与网络安全2.0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, 为发表鉴证结论提供了基础。

² 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。



独立鉴证报告 (续)

固有限制

我们提请注意，CPA Canada WebTrust电子认证-SSL证书基准审计标准与网络安全2.0版本具有某些能够影响鉴证对象信息可靠性的固有限制。

由于内部控制体系本身的限制，使其无法识别和发现所有可能发生的错误或舞弊。以及由于系统和控制、执行环境、时间、或对规章制度不同的遵循程度的变化，都可能会影响本评估报告在将来时间的参考价值。

结论

我们认为，CFCA自2014年10月1日至2015年7月31日期间的电子认证-SSL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-SSL证书基准审计标准与网络安全2.0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电子认证标识 (“WebTrust 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- SSL证书基准审计标准与网络安全2.0版本以外的质量标准声明，或对任何客户对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

2015/BJ-117/ATL/RYE

(第3页/共3页)

独立鉴证报告(续)

使用和分发限制

本报告仅供CFCA管理层根据WebTrust电子认证-SSL证书基准审计标准与网络安全2.0版本的要求，为获得WebTrust电子认证标识而向有关机构提交，不适用于任何其他目的。除了将本报告副本提供给WebTrust以外，本报告非为其他目的编制，也不能为其他目的分发或使用。

普华永道中天会计师事务所（特殊普通合伙）北京分所

2015年10月16日

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, 2015

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 October 1st, 2014 through July 31, 2015.

The management of China Financial Certification Authority Co., Ltd. (CFCA) has assessed the disclosure of its certificate practices and its controls over its CA - SSL services located at Mainland China, during the period from October 1, 2014 through July 31, 2015. 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 - SSL services at Mainland China, CFCA, during the period from October 1, 2014 through July 31, 2015, CFCA:

- 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:
 - 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 activities performed by the CA) and verified;
 - The integrity of keys and certificates it manages was established and protected throughout their 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 and performed 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.

[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
CFCA OV OCA	Signing Key	RSA 2048 bits	SHA-256	46 b0 ae c9 33 a6 26 f6 73 ba fb 74 41 c9 58 69 ea 94 31 46	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

2015年7月31日

致: 普华永道中天会计师事务所职业会计师:

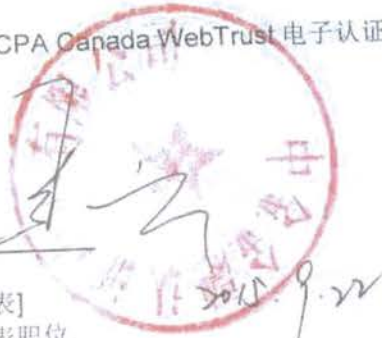
中金金融认证中心有限公司管理层就2014年10月1日至2015年7月31日,对电子认证—SSL证书业务规则披露和电子认证运行控制活动的管理层认定报告(本中文报告仅作参考,正文请参阅英文报告。)

中金金融认证中心(CFCA)管理层就在中国大陆提供的WebTrust电子认证—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,自2014年10月1日至2015年7月31日期间就CFCA提供的WebTrust电子认证—SSL证书服务,CFCA:

- 已披露 WebTrust 电子认证—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 SSL 证书在生命周期中的完整性;
 - 仅授权人员可访问 CA 系统和数据(逻辑访问及物理访问);
 - 维护密钥与证书管理的连续性;
 - 对 CA 的系统开发、维护、运行经过适当授权和操作以维护 CA 系统的完整性;
 - 对 CA 的网络系统及证书系统的安全进行了有效维护。

以符合 AICPA/CPA Canada WebTrust 电子认证-SSL 证书基准审计标准与网络安全 2.0 版本

[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
CFCA OV OCA	Signing Key	RSA 2048 bits	SHA-256	46 b0 ae c9 33 a6 26 f6 73 ba fb 74 41 c9 58 69 ea 94 31 46	CFCA EV ROOT