pwc 普华永道

INDEPENDENT ASSURANCE REPORT

2015/BJ-116/ATL/RYE

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 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 Trust Service Principles and Criteria for Certification Authorities Version 2.0. CFCA's management is responsible for the preparation and presentation of the management's assertion in accordance with the Trust Service Principles and Criteria for Certification Authorities 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 Seal on its website[1], 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 complies in all material respects with the Trust Service Principles and Criteria for Certification Authorities 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.*

INDEPENDENT ASSURANCE REPORT (Continued)

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 Trust Service Principles and Criteria for Certification Authorities 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 Trust Service Principles and Criteria for Certification Authorities Version 2.0. Within the scope of our work we performed amongst others the following procedures: (1) obtaining an understanding of CFCA's key and certificate life cycle management business and information privacy practices and procedures, and its controls over key and certificate integrity, over the authenticity and privacy of subscriber and relying party information, over the continuity of key and certificate life cycle management operations and over development, maintenance, and operation of system integrity, (2) selectively testing transactions executed in accordance with disclosed key and certificate lifecycle management business and information privacy practices, (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 Trust Service Principles and Criteria for Certification Authorities 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 October 1st, 2014 to July 31st, 2015, complies in all material respects with the Trust Service Principles and Criteria for Certification Authorities Version 2.0.

INDEPENDENT ASSURANCE REPORT (Continued)

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 Trust Service Principles and Criteria for Certification Authorities 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.

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 Trust Service Principles and Criteria for Certification Authorities 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

PricewaterhouseCoopers Zhong Tian LLP, Beijing Branch

Beijing, the people's republic of China

October 16, 2015

普华永道

独立鉴证报告

2015/BJ-116/ATL/RYE

（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服务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－增强验证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Webtrust电子认证服务原则与标准2.0版本（"Trust Service Principles and Criteria for Certification Authorities Version 2.0"）的规定设计了操作规范和业务流程。按照Webtrust电子认证服务原则与标准2.0版本编制和列报电子认证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-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。

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，供贵公司为获得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电子认证服务的管理层认定是否在所有重大方面符合Webtrust电子认证服务原则与标准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Webtrust电子认证服务原则与标准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Webtrust电子认证服务原则与标准2.0版本。在我们的鉴证工作范围内，我们实施了包括：(1)了解CFCA的电子证书生命周期管理、信息保密、遗迹密钥和证书的管理，用户和依赖方信息的鉴定和保密，密钥和证书生命周期管理的持续性，和系统在开发、变更和运行过程中的完整性；(2)评估操作规范和业务流程的设计是否遵守了披露的密钥和证书生命周期的管理，以及相关信息保密的业务规则；(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）

2015/BJ-116/ATL/RYE

固有限制

我们提请注意，Webtrust电子认证服务原则与标准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-增强验证证书服务的管理层认定在所有重大方面符合Webtrust电子认证服务原则与标准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电子认证服务原则与标准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。

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电子认证服务原则与标准2.0版本，为获得WebTrust增强验证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 Business Practices and its Controls Over its Certification Authority Operations during the period from October 1st, 2014 through July 31, 2015

China Financial Certificate Authority operates as a Certification Authority ("CFCA"). CFCA as a root CA, provides the following certification authority services:

- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate status information processing

CFCA makes use of external registration authorities for its certificates, and relies on external registration authority on subscriber information authentication and registration.

Management of CFCA is responsible for establishing and maintaining effective controls over its Certification Authority operations, including CA business practice disclosure, CA service integrity (including key and certificate lifecycle management controls), and CA environmental controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls including the possibility of human error and the circumvention or overriding controls. Accordingly, even effective internal controls can provide only reasonable assurance with respect to CFCA's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

The management of China Financial Certification Authority Co,. Ltd. (CFCA) has assessed the controls over its CA operations. 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 services at Mainland China during the period from October 1st, 2014 through July 31, 2015, CFCA:

- Disclosed its key and certificate lifecycle management business and information privacy practices and provided such services in accordance with its disclosed practices.
- Maintained effective controls to provide reasonable assurance that:
    - Subscriber information was properly authenticated (for the registration activities performed by CFCA); and

- The integrity of keys and certificates it managed was established and protected throughout their lifecycles;

- Maintained effective controls to provide reasonable assurance that:
  - Subscriber and relying party information was restricted to authroised individuals and protected from uses not specified in the CA's business practice disclosure;
  - The continuity of key and certificate lifecycle management operations was maintained; and
  - CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity

in accordance with Trust service Principles and Criteria for Certification Authorities Veersion 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
CFCA OV CodeSign OCA	Signing Key	RSA 2048 bits	SHA-256	b9 f6 7e 7f af c7 ed 03 84 ce 2e e1 2e 99 ce 1f a0 5d 65 1d	CFCA EV ROOT
CFCA EV CodeSign OCA	Signing Key	RSA 2048 bits	SHA-256	f9 f1 12 d9 ed 39 3b ec d1 71 5f 80 8a bf 3c 09 bc cd e1 8c	CFCA EV ROOT
CFCA EV SM2 Root	Root Key	256 bits	SM 2	eb b9 2e 44 11 6b 88 0a bc 94 c8 21 5b ed 81 b2 b4 fd 84 8c	CFCA EV SM2 Root
CFCA EV SM2 OCA	Signing Key	256 bits	SM 2	d0 f6 9e 6b e5 73 eb 19 c5 77 5a 9a 3b b8 e3 d4 31 8d 6a 96	CFCA EV SM2 Root
CFCA OV SM2 OCA	Signing Key	256 bits	SM 2	29 d4 ce f2 75 21 36 c1 59 3e c5 eb c1 23 d2 21 2a 3f 23 da	CFCA EV SM2 Root
CFCA OV SM2 CodeSign OCA	Signing Key	256 bits	SM 2	9f 7e 3a 7f 37 e4 41 36 e4 03 37 44 9f f3 3c 10 7c 3c 16 60	CFCA EV SM2 Root
CFCA EV SM2 CodeSign OCA	Signing Key	256 bits	SM 2	96 57 be ee 66 a3 e8 f9 ba 11 ca ff 49 fb c0 dd b9 a4 d9 da	CFCA EV SM2 Root

Key name	Key type	Key size	Algorithm	Certificates (thumbprint)	Certificates Signed by The key
CFCA GT CA	Root Key	RSA 2048 bits	SHA-1	ea bd a2 40 44 0a bb d6 94 93 0a 01 d0 97 64 c6 c2 d7 79 66	CFCA GT CA
CFCA OCA2	Signing key	RSA 2048 bits	SHA-1	6f f5 bc da 29 0b a6 d9 2c 6e 8c e7 2d 58 b7 a8 61 76 44 88	CFCA GT CA
CFCA GT SM2 CA	Root Key	256 bits	SM 2	26 83 a4 b3 fb 4c 2b 3a 66 49 54 63 62 16 df fe 96 d5 73 00	CFCA GT SM2 CA
CFCA SM2 OCA2	Singing Key	256 bits	SM 2	cc 97 16 26 7b 61 f8 d9 d8 a9 e8 0f 1d fe 8f a0 29 05 94 00	CFCA GT SM2 CA

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（简称“CFCA”）是一家提供电子认证服务的机构。做一家根CA机构，CFCA提供以下CA服务：

- 用户注册
- 电子证书更新
- 电子证书密钥更新
- 电子证书颁发
- 电子证书发布
- 电子证书撤销
- 电子证书状态信息处理

CFCA设有外部注册机构协助其进行用户信息鉴定和注册。

CFCA管理层负责建立和维护有效的控制体系来管理CA业务，包括CA规则披露、CA服务完整性（包括密钥和证书生命周期管理控制）、及CA环境控制。这些控制包含监控机制，和对问题的解决方法。

任何控制机制都存在自身的局限性，如认为失误和越权操作。因此，即使是有效的控制也仅能对CFCA的日常运行提供合理的保障。此外，控制的有效性也可能随着环境的变化而变更。

中金金融认证中心（CFCA）管理层就在中国大陆提供的WebTrust电子认证业务控制活动已进行了评估。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2014年10月1日至2015年7月31日CFCA提供的WebTrust电子认证服务，CFCA：

- 已披露密钥和证书生命周期管理，以及相关信息保密业务规则，并遵循所披露的业务规则提供电子认证服务；

- 通过有效控制机制，以提供以下合理保证：
  - 对用户信息进行适当鉴定（针对由 CFCA 操作的用户注册活动）；及
  - CFCA 管理的密钥及电子证书在其生命周期内受到妥善的保护；

- 通过有效控制机制，以提供以下合理保证：
  - 用户及相关依赖方的信息智能被获授权的人员所获取，并限制其不被用于CA业务规则生命以外的用途；
  - 持续有效的维护密钥与电子证书生命周期的管理和控制；及
  - 对CA系统的开发、维护、及运作执行适当的授权和管理，以保障其完整性。

以符合 WebTrust 电子认证服务原则与标准 2.0 版本。

2015.9.22

[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
CFCA OV CodeSign OCA	Signing Key	RSA 2048 bits	SHA-256	b9 f6 7e 7f af c7 ed 03 84 ce 2e e1 2e 99 ce 1f a0 5d 65 1d	CFCA EV ROOT
CFCA EV CodeSign OCA	Signing Key	RSA 2048 bits	SHA-256	f9 f1 12 d9 ed 39 3b ec d1 71 5f 80 8a bf 3c 09 bc cd e1 8c	CFCA EV ROOT
CFCA EV SM2 Root	Root Key	256 bits	SM 2	eb b9 2e 44 11 6b 88 0a bc 94 c8 21 5b ed 81 b2 b4 fd 84 8c	CFCA EV SM2 Root
CFCA EV SM2 OCA	Signing Key	256 bits	SM 2	d0 f6 9e 6b e5 73 eb 19 c5 77 5a 9a 3b b8 e3 d4 31 8d 6a 96	CFCA EV SM2 Root
CFCA OV SM2 OCA	Signing Key	256 bits	SM 2	29 d4 ce f2 75 21 36 c1 59 3e c5 eb c1 23 d2 21 2a 3f 23 da	CFCA EV SM2 Root
CFCA OV SM2 CodeSign OCA	Signing Key	256 bits	SM 2	9f 7e 3a 7f 37 e4 41 36 e4 03 37 44 9f f3 3c 10 7c 3c 16 60	CFCA EV SM2 Root
CFCA EV SM2 CodeSign OCA	Signing Key	256 bits	SM 2	96 57 be ee 66 a3 e8 f9 ba 11 ca ff 49 fb c0 dd b9 a4 d9 da	CFCA EV SM2 Root

Key name	Key type	Key size	Algorithm	Certificates (thumbprint)	Certificates Signed by The key
CFCA GT CA	Root Key	RSA 2048 bits	SHA-1	ea bd a2 40 44 0a bb d6 94 93 0a 01 d0 97 64 c6 c2 d7 79 66	CFCA GT CA
CFCA OCA2	Signing key	RSA 2048 bits	SHA-1	6f f5 bc da 29 0b a6 d9 2c 6e 8c e7 2d 58 b7 a8 61 76 44 88	CFCA GT CA
CFCA GT SM2 CA	Root Key	256 bits	SM 2	26 83 a4 b3 fb 4c 2b 3a 66 49 54 63 62 16 dffe 96 d5 73 00	CFCA GT SM2 CA
CFCA SM2 OCA2	Singing Key	256 bits	SM 2	cc 97 16 26 7b 61 f8 d9 d8 a9 e8 0f 1d fe 8f a0 29 05 94 00	CFCA GT SM2 CA