pwc

普华永道

Shanghai Electronic Certificate Authority Center Co., Ltd.
18th Floor
No. 1717 North Sichuan Rd.
Shanghai
China

2015/SH-184/CCYI/MWJ

Report of Independent Accountant on Assessment of the Assertion by the management of Shanghai Electronic Certificate Authority Center Co., Ltd. ("SHECA")

To: Mr. Li Guo
General Manager, Shanghai Electronic Certificate Authority Center Co., Ltd.

We have been engaged to perform a reasonable assurance engagement on the accompanying assertion by the management of Shanghai Electronic Certificate Authority Center Co., Ltd. ("SHECA") for the period 1st May 2014 through 30th April 2015, for its Certification Authority ("CA") - Extended Validation ("EV") operations, SHECA has:

- Disclosed its Extended Validation (EV) Code Signing and EV SSL certificate life cycle management practices and procedures, including its commitment to provide EV Code Signing and EV SSL certificates in conformity with the CA/Browser Forum Guidelines and provided such services in accordance with its disclosed practices;

- Maintained effective controls to provide reasonable assurance that:
  - EV Code Signing and EV SSL Subscriber information was properly collected, authenticated (for the registration activities performed by SHECA) and verified; and
  - the integrity of keys and EV Code Signing and EV SSL certificates it manages was established and protected throughout their life cycles.

in accordance with the CPA Canada WebTrust Principles and Criteria for Certification Authorities – Extended Validation Code Signing, and Trust Services Principles and Criteria for Certification Authorities – Extended Validation SSL – Version 1.4.5.

Management's Responsibility for the Management's Assertion of SHECA

SHECA's management is responsible for the preparation and presentation of the management's assertion in accordance with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation Code Signing, and Trust Services Principles and Criteria for Certification Authorities – Extended Validation SSL– Version 1.4.5. This responsibility includes designing, implementing and maintaining internal control relevant to the preparation and presentation of the management's assertion of SHECA and 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 SHECA 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 the management to submit to the related authority to continue displaying the WebTrust EV 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.

The relative effectiveness and significance of specific controls at SHECA 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 have performed no procedures to evaluate the effectiveness of controls at individual subscribers and relying party locations.

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 whether the management's assertion of SHECA complies, in all material respects, with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation Code Signing, and Trust Services Principles and Criteria for Certification Authorities – Extended Validation SSL – Version 1.4.5.

A reasonable assurance engagement involves performing procedures to obtain sufficient appropriate evidence whether the management's assertion of SHECA complies with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation Code Signing, and Trust Services Principles and Criteria for Certification Authorities – Extended Validation SSL – Version 1.4.5. The procedures selected depend on the auditor's judgment, including the assessment of the risks of material noncompliance of the management's assertion of SHECA with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation Code Signing, and Trust Services Principles and Criteria for Certification Authorities – Extended Validation SSL – Version 1.4.5. Within the scope of our work, we performed amongst others the following procedures: (1) obtaining an understanding of SHECA EV certificate life cycle management practices and procedures, including its relevant

[1] *The maintenance and integrity of the SHECA 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 respoonsibility for any differences between the accompanying assertion by the management of SHECA on which the assurance report was issued or the assurance report that was issued and the information presented on the website.*

controls over the issuance, renewal and revocation of EV certificates; (2) selectively testing transactions executed in accordance with disclosed key and certificate life cycle management business and information privacy 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 conclusion.

Inherent Limitation

We draw attention to the fact that the WebTrust Principles and Criteria for Certification Authorities – Extended Validation Code Signing, and Trust Services Principles and Criteria for Certification Authorities – Extended Validation SSL – Version 1.4.5 include certain inherent limitations that can influence the reliability of the information.

Because of inherent limitations in controls, errors or fraud may occur and not be 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 assertion by the management of SHECA for the period 1st May 2014 through 30th April 2015 complies, in all material respects, with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation Code Signing, and Trust Services Principles and Criteria for Certification Authorities – Extended Validation SSL – Version 1.4.5.

Emphasis of Matters

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

SHECA's use of the WebTrust for Certification Authorities – Extended Validation Seal 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.

This report does not include any representation as to the quality of SHECA's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – Extended Validation Code Signing, and Trust Services Principles and

Criteria for Certification Authorities – Extended Validation SSL – Version 1.4.5, or the suitability of any of SHECA's services for any customer's intended purpose.

Restriction on Use and Distribution

Our report is intended solely for the use of SHECA to submit the report to the related authority in connection with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation Code Signing, and Trust Services Principles and Criteria for Certification Authorities – Extended Validation SSL – Version 1.4.5 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
普华永道中天会计师事务所（特殊普通合伙）

PricewaterhouseCoopers Zhong Tian LLP

Shanghai, China
5 June 2015

上海市数字证书认证中心有限公司
中国上海市
四川北路 1717 号 18 楼

2015/SH-184/CCYI/MWJ

上海市数字证书认证中心有限公司WebTrust电子认证—增强验证资格独立鉴证报告
（注意：本中文报告只作参考。正文请参阅英文报告。）

致：上海市数字证书认证中心有限公司总经理李国先生

我们接受委托，对后附的上海市数字认证中心有限公司（Shanghai Electronic Certificate Authority Centre Co., Ltd.，简称“SHECA”）于 2014 年 5 月 1 日至 2015 年 4 月 30 日止期间电子认证—增强验证服务的管理层认定执行了合理保证的鉴证业务。根据管理层认定，SHECA：

- 披露 WebTrust 电子认证—代码签名增强验证及 WebTrust 电子认证—SSL 增强验证的业务实践和程序，包括承诺遵循 CA/Browser 论坛的相关指引提供 EV 代码签名证书及 EV 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：
  - 恰当的收集、鉴定（SHECA 所执行的注册操作）和验证 EV 代码签名及 EV SSL 证书申请者的信息；及
  - 有效维护密钥与 EV 代码签名及 EV SSL 证书在生命周期中的完整性。

以符合 CPA Canada WebTrust Principles and Criteria for Certification Authorities – Extended Validation Code Signing（“WebTrust 电子认证—代码签名增强验证审计标准”）及 Trust Services Principles and Criteria for Certification Authorities – Extended Validation SSL Version 1.4.5（“ WebTrust 电子认证—SSL 增强验证审计标准”）。

管理层对电子认证—代码签名增强验证服务、SSL 增强验证服务管理层认定的责任

根据WebTrust电子认证—代码签名增强验证审计标准及WebTrust电子认证—SSL增强验证审计标准的规定，按照WebTrust电子认证—代码签名增强验证审计标准及WebTrust电子认证—SSL增强验证审计标准编制和列报电子认证—增强验证服务的管理层认定是SHECA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—代码签名增强验证服务和电子认证—SSL增强验证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

根据WebTrust电子认证—代码签名增强验证审计标准及WebTrust电子认证—SSL增强验证审计标准的规定，我们的职责是在执行鉴证工作的基础上对 SHECA 电子认证—代码签名增强验证服务和电子认证—SSL 增强验证服务的管理层认定发表结论，并按照双方同意的业务规定条款，仅对贵方报告我们的结论，供贵方根据 WebTrust 电子认证—代码签名增强验证审计标准及 WebTrust 电子认证—SSL 增强验证审计标准的要求，为持续获得 WebTrust Extended Validation 电子认证标识（“WebTrust EV Seal[1]”）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或义务。

SHECA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SHECA电子认证—增强验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—代码签名增强验证审计标准及WebTrust电子认证—SSL增强验证审计标准获取合理保证。

合理保证的鉴证工作及实施鉴证程序，以获取有关SHECA电子认证—增强验证服务的管理层认定是否符合WebTrust电子认证—代码签名增强验证审计标准及WebTrust电子认证—SSL增强验证审计标准的充分适当的证据。选择的鉴证程序取决于审计师的判断，包括对SHECA电子认证—代码签名增强验证服务和电子认证—SSL增强验证服务的管理层认定存在重大不符合WebTrust电子认证—代码签名增强验证审计标准及WebTrust电子认证—SSL增强验证审计标准风险的评估。在我们的鉴证工作范围内，我们实施了包括：（1）了解SHECA增强验证证书生命周期管理，包括增强验证证书发放、更新和吊销等相关控制；（2）测试业务操作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）测试和评估控制活动执行的有效性；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。

固有限制

我们提请注意，WebTrust电子认证—代码签名增强验证审计标准及WebTrust电子认证—SSL增强验证审计标准具有某些能够影响鉴证对象信息可靠性的固有限制。

[1] *SHECA 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SHECA 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。*

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和舞弊。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，都有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，SHECA于2014年5月1日至2015年4月30日止期间电子认证—增强验证电子认证服务的管理层认定在所有重大方面符合WebTrust电子认证—代码签名增强验证审计标准及WebTrust电子认证—SSL增强验证审计标准。

强调事项

在不影响我们结论的前提下，我们提请注意：

在SHECA网站上的WebTrust EV电子认证标识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。

本报告并不包括任何在WebTrust电子认证—代码签名增强验证审计标准及WebTrust电子认证—SSL增强验证审计标准以外的质量标准声明，或对任何客户对SHECA服务的合适性声明。

使用和分发限制

本报告仅供 SHECA 根据 WebTrust 电子认证—代码签名增强验证审计标准及 WebTrust 电子认证—SSL 增强验证审计标准的要求而向有关机构提交时使用，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。

PricewaterhouseCoopers Zhong Tian LLP

普华永道中天会计师事务所（特殊普通合伙）

中国上海市
2015 年 6 月 5 日

上海市数字证书认证中心有限公司

Shanghai Electronic Certificate
Authority Center Co.,Ltd
18th Floor,
No.1717, North Sichuan Rd,
Shanghai, China
Tel: (021) 36393199
Fax: (021) 36393200
http://www.sheca.com/

PricewaterhouseCoopers Zhong Tian LLP
11th Floor
PricewaterhouseCoopers Center
2 Corporate Avenue
202 Hu Bin Road, Huangpu District
Shanghai 200021, PRC

15 May 2015

Dear Sirs:

Assertion of Management as to the Disclosure to Business Practices and Controls over the Certification Authority – Extended Validation Operations during the period from 1st May 2014 through 30th April 2015.

The management of Shanghai Electronic Certificate Authority Centre Co., Ltd. ("SHECA") has assessed the disclosure of its certificate practices and its controls over its SHECA Extended Validation ("EV") Code Signing certification authority ("CA") services and Extended Validation (EV) SSL certification authority (CA) service located in China. The keys and certificates covered in our assessment are listed in the **Appendix** of this letter. Based on that assessment, in SHECA Management's opinion, SHECA in providing its EV Code Signing and SSL – CA services in China, during the period from 1st May 2014 through 30th April 2015:

- disclosed its Extended Validation (EV) Code Signing and EV SSL certificate life cycle management practices and procedures, including its commitment to provide EV Code Signing and EV SSL certificates in conformity with the CA/Browser Forum Guidelines and provided such services in accordance with its disclosed practices;

- maintained effective controls to provide reasonable assurance that:
  - EV Code Signing and EV SSL Subscriber information was properly collected, authenticated (for the registration activities performed by SHECA) and verified;
  - the integrity of keys and EV Code Signing and EV SSL certificates it manages was established and protected throughout their life cycles,

in accordance with the CPA Canada WebTrust Principles and Criteria for Certification Authorities – Extended Validation Code Signing, and Trust Services Principles and Criteria for Certification Authorities – Extended Validation SSL – Version 1.4.5 including the following:

<u>CA EV Business Practices Disclosure</u>

<u>Service Integrity</u>

Subscriber Profile

EV Certificate Content and Profile
EV Certificate Request Requirements
Information Verification Requirements
Certificates Status Checking and Revocation
Employee and Third Party Issues
Data and Record Issues

Yours faithfully

李国

Mr. Li Guo
General Manager of Shanghai Electronic Certificate Authority Center Co., Ltd.

上海市数字证书认证中心有限公司

Company Chop

Appendix

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

Key Name	Key Type	Key Size(bits)	Certificates (Thumbprint)	Signature Algorithm	Certificate Signed by the key
UCA Extended Validation Root	Root Key	4096	b9 c9 f5 8b 3b be f5 75 e2 b5 83 28 77 0e 7b 00 76 c4 0b 5e	SHA-1	UCA Extended Validation Root
			a3 a1 b0 6f 24 61 23 4a e3 36 a5 c2 37 fc a6 ff dd f0 d7 3a	SHA-256	
SHECA Extended Validation SSL CA	Signing Key	2048	ae 40 a3 74 82 a0 2b c9 48 78 67 03 93 c5 3e 86 28 6b d0 5f	SHA-1	UCA Extended Validation Root
			76 be 95 77 18 7a bc 51 d6 5d 9c eb 4b 49 16 15 f6 e0 ab c1	SHA-256	
SHECA Extended Validation Code Signing CA	Signing Key	2048	ec 24 4e 3e 2f a0 d3 61 cb c9 4d 5c f6 ba 26 6b a9 59 b3 d7	SHA-1	UCA Extended Validation Root
			b7 9f e6 76 dc 58 3d 00 e5 8a fc 62 2f d0 c5 a4 77 fb fd 69	SHA-256	

上海市数字证书认证中心有限公司

上海市数字证书认证中心有限公司
上海市四川北路1717号18楼
200080
电话：(021) 36393199
传真：(021) 36393200
http://www.sheca.com/

普华永道中天会计师事务所（特殊普通合伙）
中国上海市黄浦区湖滨路202号
企业天地2号楼
普华永道中心11楼

2015 年 5 月 15 日

致：普华永道中天会计师事务所（特殊普通合伙）：

就 2014 年 5 月 1 日到 2015 年 4 月 30 日期间电子认证—增强验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。）

上海市数字证书认证中心有限公司（简称“SHECA”）就电子认证—代码签名增强验证和电子认证—SSL 增强验证业务规则披露和电子运行控制活动进行了评估。**附件**列示了评估所包括的密钥和证书。根据评估，SHECA 管理层认为， SHECA 在 2014 年 5 月 1 日至 2015 年 4 月 30 日就 SHECA 提供的 WebTrust 电子认证—代码签名增强验证服务和 WebTrust 电子认证—SSL 增强验证服务期间，SHECA：

- 披露 WebTrust 电子认证—代码签名增强验证及 WebTrust 电子认证—SSL 增强验证的业务实践和程序，包括承诺遵循 CA/Browser 论坛的相关指引提供 EV 代码签名证书及 EV 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：
  - 恰当的收集、鉴定（SHECA 所执行的注册操作）和验证 EV 代码签名及 EV SSL 证书申请者的信息；及
  - 有效维护密钥与 EV 代码签名及 EV SSL 证书在生命周期中的完整性

以符合CPA Canada WebTrust电子认证—代码签名增强验证审计标准及WebTrust电子认证—SSL增强验证审计标准，包含：

<u>业务规则披露</u>

<u>服务完整性</u>
订户信息
增强认证内容和信息
增强认证需求
信息验证需求
证书状态验证和撤销
雇员和第三方
数据和记录

李国

李国
上海市数字证书认证中心有限公司总经理

公司盖章: ________________________________

上海市数字证书认证中心有限公司

附件

下表列示了管理层对CA的控制活动评估所包括的密钥和证书：

密钥名称	密钥种类	密钥长度（bits）	证书（Thumbprint）	签名算法	证书签发密钥
UCA Extended Validation Root	Root Key	4096	b9 c9 f5 8b 3b be f5 75 e2 b5 83 28 77 0e 7b 00 76 c4 0b 5e	SHA-1	UCA Extended Validation Root
			a3 a1 b0 6f 24 61 23 4a e3 36 a5 c2 37 fc a6 ff dd f0 d7 3a	SHA-256	
SHECA Extended Validation SSL CA	Signing Key	2048	ae 40 a3 74 82 a0 2b c9 48 78 67 03 93 c5 3e 86 28 6b d0 5f	SHA-1	UCA Extended Validation Root
			76 be 95 77 18 7a bc 51 d6 5d 9c eb 4b 49 16 15 f6 e0 ab c1	SHA-256	
SHECA Extended Validation Code Signing CA	Signing Key	2048	ec 24 4e 3e 2f a0 d3 61 cb c9 4d 5c f6 ba 26 6b a9 59 b3 d7	SHA-1	UCA Extended Validation Root
			b7 9f e6 76 dc 58 3d 00 e5 8a fc 62 2f d0 c5 a4 77 fb fd 69	SHA-256	