

INDEPENDENT PRACTITIONER'S ASSURANCE REPORT

To the management of Shanghai Electronic Certificate Authority Center Co., Ltd.

We have been engaged to perform a reasonable assurance engagement on the accompanying management's assertion of Shanghai Electronic Certificate Authority Center Co., Ltd. ("SHECA") for its Certification Authority - Extended Validation Code Signing ("EV CS") operations at Shanghai, China for the period from May 1, 2019 to April 30, 2020.

Management's Responsibilities

SHECA's management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation Code Signing – Version 1.4.1.

Our Independence and Quality Control

We have complied with the independence and other ethical requirement of the International Code of Ethics for Professional Accountants (including International Independence Standards) 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 Responsibilities

It is our responsibility to express an opinion on the accompanying assertion 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.

A reasonable assurance engagement involves performing procedures to obtain sufficient appropriate evidence whether the management assertion of SHECA is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation Code Signing – Version 1.4.1. 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)

INDEPENDENT PRACTITIONER’S ASSURANCE REPORT (CONTINUED)

obtaining an understanding of SHECA’s EV CS certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of EV CS certificates, EV CS Signing Authority certificates, and EV CS Timestamp Authority certificates; (2) selectively testing transactions executed in accordance with disclosed EV CS certificate lifecycle management practices; (3) testing and evaluating the operating effectiveness of the controls; and (4) performing such other procedures as we considered necessary in the circumstances.

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 subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

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 WebTrust Principles and Criteria for Certification Authorities – Extended Validation Code Signing – Version 1.4.1 includes certain inherent limitations that can influence the reliability of the information.

For example, controls may not prevent, or detect and correct, error, fraud, unauthorised access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

Opinion

In our opinion, the accompanying assertion of SHECA, for the period from May 1, 2019 to April 30, 2020, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation Code Signing – Version 1.4.1.

Emphasis of Matter

Without modifying our conclusion, we draw attention to the fact that 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 – Version 1.4.1, nor the suitability of any of SHECA’s services for any customer’s intended purpose.

Other Matter

INDEPENDENT PRACTITIONER’S ASSURANCE REPORT (CONTINUED)

SHECA’s use of the WebTrust for Certification Authorities 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.

Purpose and Restriction on Use

The accompanying assertion was prepared for obtaining and displaying the WebTrust Seal on SHECA website¹ using the WebTrust Principles and Criteria for Certification Authorities – Extended Validation Code Signing – Version 1.4.1 designed for this purpose. As a result, the accompanying assertion of SHECA may not be suitable for another purpose. This report is intended solely for the Management of SHECA in connection with obtaining and displaying the WebTrust Seal on its website for submission of the report to the related authority in connection with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation Code Signing – Version 1.4.1. We do not assume responsibility towards or accept liability to any other person for the contents of this report.



PricewaterhouseCoopers
Certified Public Accountants

Hong Kong, China

June 12, 2020

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 responsibility 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.

注册会计师独立鉴证报告

(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管理层

我们接受委托，对后附上海市数字证书认证中心有限公司（Shanghai Electronic Certificate Authority Center Co., Ltd.，简称“SHECA”）于 2019 年 5 月 1 日至 2020 年 4 月 30 日期间于中国上海运营的代码签名增强电子认证服务管理层认定执行了合理保证的鉴证业务。

管理层的责任

SHECA 的管理层负责确保管理层认定，包括其陈述的客观性以及认定中描述的 SHECA 所提供的服务能够符合 WebTrust 电子认证代码签名增强验证资格原则及规范 V1.4.1 的规定。

我们的独立性和质量控制

我们遵守了国际会计师职业道德准则理事会颁布的国际会计师道德守则（包括国际独立性标准）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的书面政策与程序。

注册会计师的责任

我们的责任是在执行鉴证工作的基础上对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资格原则及规范 V1.4.1 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 SHECA 代码签名增强验证证书生命周期管理，包括代码签名增强验证证书发放、更新和吊销，代码签名增强验证签名机构证书管理，以及代码签名增强验证时间戳机构证书等相关控制；（2）测试业务操作是否遵守了所披露的证书生命周期管理；（3）测试和评估控制活动执行的有效性；以及（4）执行其他我们认为必要的鉴证程序。

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。

注册会计师独立鉴证报告（续）

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。

固有限制

我们提请使用者注意，WebTrust 电子认证代码签名增强验证资格原则及规范 V1.4.1 具有某些可能影响鉴证对象信息可靠性的固有限制。

例如，控制可能不能预防，或发现和纠正错误、舞弊、未经授权访问系统和信息，或未能遵守内部和外部的政策或要求。并且，风险的变化可能会影响基于我们的发现所得出的结论在将来时间的有效性。

意见

我们认为，SHECA 于 2019 年 5 月 1 日至 2020 年 4 月 30 日期间的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资格原则及规范 V1.4.1。

强调事项

我们提请使用者关注，本报告并不包括任何在 WebTrust 电子认证代码签名增强验证资格原则及规范 V1.4.1 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。

其他事项

在 SHECA 网站上的 WebTrust 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。

目的及使用和分发限制

后附管理层认定为在 SHECA 网站¹上获取并展示 WebTrust Seal 编制，并采用为该目的而设计的 WebTrust 电子认证代码签名增强验证资格原则及规范 V1.4.1，因此后附 SHECA 管理层认定可能不适用于其他目的。本报告仅供 SHECA 管理层根据 WebTrust 电子认证代码签名增强验证资格原则及规范 V1.4.1，持续获得并在 SHECA 网站上展示 WebTrust 电子认证标识而向 WebTrust 相关机构（CPA Canada）提交的目的使用。我们不会就本报告的内容向任何其他人士负上或承担任何责任。

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。



羅兵咸永道

第 3 页/共 3 页

注册会计师独立鉴证报告（续）

罗兵咸永道会计师事务所
执业会计师

香港，2020年6月12日



Shanghai Electronic Certificate Authority Center Co.,Ltd

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

PricewaterhouseCoopers
22nd Floor
Prince's Building
Central, Hong Kong, PRC

June 12, 2020

Dear Sirs,

Assertion of Management as to the Disclosure to Business Practices and Controls over the Certification Authority - Extended Validation Code Signing Operations during the period from May 1, 2019 through April 30, 2020

Shanghai Electronic Certificate Authority Center Co., Ltd. (“SHECA”) operates the Certification Authority (CA) services known as its Root and Subordinate CAs (please refer to the appendix), and provides Extended Validation Code Signing (“EV CS”) CA services.

The management of SHECA is responsible for establishing and maintaining effective controls over its EV CS CA operations, including its EV CS CA business practices disclosure on its website, EV CS key lifecycle management controls, EV CS certificate lifecycle management controls and EV CS Timestamp Authority certificate lifecycle management 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 of controls. Accordingly, even effective controls can only provide reasonable assurance with respect to SHECA’s Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

SHECA management has assessed its disclosures of its certificate practices and controls over its EV CS CA services. Based on that assessment, in SHECA management’s opinion, in providing its EV CS Certification Authority (CA) services at Shanghai, China, throughout the period May 1, 2019 to April 30, 2020, SHECA has:

- disclosed its EV CS certificate lifecycle management business practices in its:
 - UniTrust EV Certification Practice Statement Version 1.4.6 (<https://assets-cdn.sheca.com/documents/unitrust-ev-certification-practice-statement-en-v1.4.6.pdf>);
 - UniTrust EV Certification Practice Statement Version 1.4.5;
 - UniTrust EV Certification Practice Statement Version 1.4.4;
 - UniTrust EV Certification Practice Statement Version 1.4.3; and
 - UniTrust EV Certificate Policy Version 1.6.3 (<https://assets-cdn.sheca.com/documents/unitrust-ev-certification-policy-version-1.6.3.pdf>);

cdn.sheca.com/documents/unitrust-ev-certificate-policy-en-v1.6.3.pdf);

- UniTrust EV Certificate Policy Version 1.6.2;
 - UniTrust EV Certificate Policy Version 1.6.1;
 - UniTrust EV Certificate Policy Version 1.6, including its commitment to provide EV CS certificates in conformity with the CA/Browser Forum Guidelines on the SHECA website, and provided such services in accordance with its disclosed practices
- maintained effective controls to provide reasonable assurance that:
 - the integrity of keys and EV CS certificates it manages is established and protected throughout their lifecycles; and
 - EV CS subscriber information is properly authenticated (for the registration activities performed by SHECA)
 - maintained effective controls to provide reasonable assurance that:
 - requests for EV CS Timestamp Authority certificates are properly authenticated; and
 - certificates issued to EV CS Timestamp Authorities are not valid for a period longer than specified by the CA/Browser Forum

in accordance with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation Code Signing – Version 1.4.1 (<https://www.epacanada.ca/-/media/site/business-and-accounting-resources/docs/webtrust/wt-pcca-evcs-1-4-1.pdf?la=en&hash=1BEE0463EF83CBE538582376B4AC8DE5DBA30C6C>).



Mr. Cui Jiuqiang
General Manager of Shanghai Electronic Certificate Authority Center Co., Ltd.



Appendix

The list of keys and certificates covered in the management's assertion is as follow:

Key Name	Key Type	Signature Algorithm	Key Size	Subject Key Identifier	Certificates (Thumbprint)	Certificate Signed by
UCA Extended Validation Root	Root Key	sha256RSA	4096 bits	d9 74 3a e4 30 3d od f7 12 dc 7e 5a 05 9f 1e 34 9a f7 e1 14	D43AF9B35473755 C9684FC06D7D8C B70EE5C28E773FB 294EB41EE7172292 4D24	UCA Extended Validation Root
SHECA Extended Validation Code Signing CA	Signing Key	sha256RSA	2048 bits	74 98 99 6f 6a 15 c0 06 25 20 85 1c af 2b 31 6b 87 ed a3 db	A392C645B9A5AD 6A214F19DE77634 6BC7DD6BB15818E 433886DAC54EE66 61852	UCA Extended Validation Root
SHECA RSA Extended Validation Code Signing CA	Signing Key	sha256RSA	2048 bits	8e 40 66 5f 6a a9 40 c2 b9 f1 fo 4a 22 63 95 64 59 37 07 e5	D404FAFA4BA2F4 26B66CD219C6DA 84F91CoFB7CB584 29EC8077E2A7643 14D55D	UCA Extended Validation Root
UniTrust Global Root CA R1	Root Key	sha384RSA	4096 bits	3c a0 61 b0 ef da c6 e8 bb 2d e1 56 a2 eb bb b6 3d 23 23 81	81B35EFC42C7794 7209D76B51B5E7B 122CE78348AE8C4 525DC8D4B30289 E5385	UniTrust Global Root CA R1
UniTrust Global Root CA R2	Root Key	sha384ECDSA	384 bits	e4 53 66 b7 b7 a4 e9 d7 cc c1 21 e0 4a cf cc ac 01 bc 72 bc	78919B35D1C61559 5A51328A5C54608 3B4D5320724A258 695B991F2F61C4D CC7	UniTrust Global Root CA R2



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 电话：
(021) 36393199
传真：(021) 36393200
<http://www.sheca.com/>

罗兵咸永道会计师事务所
中国香港
中环太子大厦22楼

2020年6月12日

致：罗兵咸永道会计师事务所

就**2019年5月1日到2020年4月30日**期间代码签名增强验证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。)

上海市数字证书认证中心有限公司 (Shanghai Electronic Certificate Authority Center Co., Ltd., 简称“SHECA”) 运营电子认证服务机构，并提供代码签名增强验证电子认证服务，附件列示了服务所包括的根证书和中级证书。

SHECA 的管理层负责针对代码签名增强验证服务建立并维护有效的控制，包括：披露代码签名增强验证业务规则，代码签名增强验证密钥生命周期管理，代码签名增强验证证书生命周期管理和代码签名增强验证时间戳服务证书生命周期管理。这些控制包括监控机制及为纠正已识别的缺陷所采取的改进措施。

任何控制都有其固有限制，包括人为失误，以及规避或逾越控制的可能性。因此，即使有效的控制也仅能对 SHECA 运营的电子认证服务提供合理保证。此外，由于控制环境的变化，控制的有效性可能随时间而发生变化。

SHECA 管理层已对证书业务披露和代码签名增强验证电子认证服务控制进行评估。基于此评估，SHECA 管理层认为，在 2019 年 5 月 1 日至 2020 年 4 月 30 日就 SHECA 在中国上海提供的代码签名增强验证电子认证服务期间，SHECA:

- 披露代码签名增强验证证书生命周期管理业务规则于：
 - UniTrust EV 证书电子认证业务规则 V 1.4.6 (<https://assets-cdn.sheca.com/documents/unitrust-ev-certification-practice-statement-cn-v1.4.6.pdf>) ；
 - UniTrust EV 证书电子认证业务规则 V 1.4.5；
 - UniTrust EV 证书电子认证业务规则 V 1.4.4；
 - UniTrust EV 证书电子认证业务规则 V 1.4.3； 以及
 - UniTrust EV 证书策略 V 1.6.3 (<https://assets-cdn.sheca.com/documents/unitrust-ev-certificate-policy-cn-v1.6.3.pdf>) ；
 - UniTrust EV 证书策略V 1.6.2；
 - UniTrust EV 证书策略V 1.6.1；

- UniTrust EV 证书策略V 1.6。
包括承诺遵循CAB论坛（CA/Browser Forum）的相关指引提供代码签名增强验证服务，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：
 - 有效维护密钥与代码签名增强验证证书在生命周期中的完整性；以及
 - 恰当地鉴定（SHECA所执行的注册操作）代码签名增强验证证书申请者的信息。
- 通过有效控制机制，以提供以下合理保证：
 - 代码签名增强验证时间戳证书的申请是恰当鉴定的；以及
 - 代码签名增强验证时间戳服务签发的证书有效期不会比CAB论坛（CA/Browser Forum）的规定时间长。

以符合 WebTrust 电子认证代码签名增强验证审计标准 V1.4.1（WebTrust Principles and Criteria for Certification Authorities - Extended Validation Code Signing – Version 1.4.1）（<https://www.cpacanada.ca/-/media/site/business-and-accounting-resources/docs/webtrust/wt-pcca-evcs-1-4-1.pdf?la=en&hash=1BEE0463EF83CBE538582376B4AC8DE5DBA30C6C>）。

崔久强
上海市数字证书认证中心有限公司总经理

公司盖章

附件

下表列示本认定报告所包括的密钥和证书：

密钥名称	密钥种类	密钥算法	密钥长度	密钥 ID	证书指纹	证书签发者
UCA Extended Validation Root	Root Key	sha256RSA	4096 bits	d9 74 3a e4 30 3d od f7 12 dc 7e 5a 05 9f 1e 34 9a f7 e1 14	D43AF9B35473755 C9684FC06D7D8C B70EE5C28E773FB 294EB41EE7172292 4D24	UCA Extended Validation Root
SHECA Extended Validation Code Signing CA	Signing Key	sha256RSA	2048 bits	74 98 99 6f 6a 15 c0 06 25 20 85 1c af 2b 31 6b 87 ed a3 db	A392C645B9A5AD 6A214F19DE77634 6BC7DD6BB15818E 433886DAC54EE66 61852	UCA Extended Validation Root
SHECA RSA Extended Validation Code Signing CA	Signing Key	sha256RSA	2048 bits	8e 40 66 5f 6a a9 40 c2 b9 f1 fo 4a 22 63 95 64 59 37 07 e5	D404FAFA4BA2F4 26B66CD219C6DA 84F91CoFB7CB584 29EC8077E2A7643 14D55D	UCA Extended Validation Root
UniTrust Global Root CA R1	Root Key	sha384RSA	4096 bits	3c a0 61 bo ef da c6 e8 bb 2d e1 56 a2 eb bb b6 3d 23 23 81	81B35EFC42C7794 7209D76B51B5E7B 122CE78348AE8C4 525DC8D4B30289 E5385	UniTrust Global Root CA R1
UniTrust Global Root CA R2	Root Key	sha384ECDSA	384 bits	e4 53 66 b7 b7 a4 e9 d7 cc c1 21 e0 4a cf cc ac 01 bc 72 bc	78919B35D1C61559 5A51328A5C54608 3B4D5320724A258 695B991F2F61C4D CC7	UniTrust Global Root CA R2