pwc 羅兵咸永道

Independent practitioner's assurance report

To the management of Shanghai Electronic Certificate Authority Co., Ltd. ("SHECA")

Scope

We have been engaged to perform a reasonable assurance engagement on the accompanying management's assertion of SHECA for its Certification Authority (CA) operations at Shanghai (including Facility 1 and Facility 2), China for the period from April 1, 2023 to March 31, 2024 for its CAs enumerated in the Attachment A, SHECA has:

- disclosed its extended validation SSL ("EV SSL") certificate lifecycle management business practices in its:
  - UniTrust EV Certification Practice Statement v1.5.5;
  - UniTrust EV Certification Practice Statement v1.5.4;
  - UniTrust EV Certification Practice Statement v1.5.3;
  - UniTrust EV Certification Practice Statement v1.5.2;
  - UniTrust EV Certificate Policy Version 1.7.1;
  - UniTrust EV Certificate Policy Version 1.7.0;
  - UniTrust EV Certificate Policy Version 1.6.9; and
  - UniTrust EV Certificate Policy Version 1.6.8,

  including its commitment to provide EV SSL 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 SSL certificates it manages is established and protected throughout their lifecycles; and
  - EV SSL subscriber information is properly authenticated (for the registration activities performed by SHECA),

in accordance with the WebTrust Principles and Criteria for Certification Authorities - Extended Validation SSL v1.8.

Management's Responsibilities

SHECA's management is responsible for the management's 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 SSL v1.8.

Our Independence and Quality Management

We have complied with the independence and other ethical requirements 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 Management 1, which requires the firm to design, implement and operate a system of quality management including policies or 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 management's assertion based on our work performed.

We conducted our work in accordance with 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's assertion of SHECA is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities - Extended Validation SSL v1.8. 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 SHECA's EV SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of EV SSL certificates; (2) selectively testing transactions executed in accordance with disclosed EV SSL 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

Because of the nature and inherent limitations of controls, SHECA's ability to meet the aforementioned criteria may be affected. 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 opinion based on our findings to future periods is subject to the risk that changes may alter the validity of such opinion.

pwc 羅兵咸永道

Opinion

In our opinion, the management's assertion of SHECA, for the period from April 1, 2023 to March 31, 2024, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities - Extended Validation SSL v1.8.

Emphasis of Matter

Without modifying our opinion, 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 SSL v1.8, nor the suitability of any of SHECA's services for any customer's intended purpose.

Other Matter

The UniTrust Global Root CA R1 (Attachment A #11), UniTrust Global Root CA R2 (Attachment A #13) CAs did not issue certificates during the period April 1, 2023 to March 31, 2024 and were maintained online to provide revocation status information only.

SHECA's management has disclosed 10 incidents (see Attachment B) during the period from April 1, 2023 to March 31, 2024. The remedial actions and the root causes of these incidents undertaken by SHECA have been posted publicly in the online forums of the Bugzilla site, as well as the online forums of individual internet browsers that comprise the CA/Browser Forum.

Purpose and Restriction on Use

The management's assertion was prepared for obtaining and displaying the WebTrust Seal on SHECA website[1] using the WebTrust Principles and Criteria for Certification Authorities - Extended Validation SSL v1.8 designed for this purpose. As a result, the management's 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 after submitting the report to the related authority in connection with the WebTrust Principles and Criteria for Certification Authorities - Extended Validation SSL v1.8.

Our report is not to be used for any other purpose. We do not assume responsibility towards or accept liability to any other parties for the contents of this report.

Use of the WebTrust seal

---

[1] *The maintenance and integrity of the SHECA website is the responsibility of the management of SHECA; 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 management's assertion of SHECA on which the assurance report was issued or the assurance report that was issued and the information presented on the website.*

羅兵咸永道

SHECA's use of the WebTrust for Certification Authorities - Extended Validation SSL 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.

PricewaterhouseCoopers
Certified Public Accountants

Hong Kong, 24 May 2024

pwc

羅兵咸永道

Attachment A

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

#	Key Name	Key Type	Signature Algorithm	Key Size	Subject DN	Subject Key Identifier	Certificates Thumbprint (SHA256)	Certificate Signed by
1	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	9BEA11C976FE014764C1BE56A6F914B5A5600317ABD9988393382E5161AA0493C	UCA Global G2 Root
2	SHECA EV Server CA G2	Signing Key	sha256RSA	2048 bits	CN = SHECA EV Server CA G2 O = UniTrust C = CN	86B148C0420A9C6F81FC4FDCD10F184BAAB5A6EA	4216527163AD2CAA825D3BF48F61A7661D0ABC89B58AB76B23A1E10999F0769F	UCA Global G2 Root
3	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	C1AFC65B1E813B0E6146E6AA5341681272ABE9A38D59F7BD1B27B729834A0D9C	Certum Trusted Network CA
4	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	3DD69C5BE170F943F804D1D31FE8F916C0C0226CDDD7AEA9AA9A0CDFD3474361	Certum Trusted Network CA
5	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	BB61408AED9F530B2EC0545E53BA2C8EBEAA57D9976447DB1663CED4600CD6B7	Certum Trusted Network CA
6	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	BFA95C5DF164B659FA32F6D10564D7170DDE661A853A782E6AB63639433BCB41	Certum Trusted Network CA
7	UCA Extended Validation Root	Root Key	sha256RSA	4096 bits	CN = UCA Extended Validation Root O = UniTrust C = CN	D9743AE4303D0DF712DC7E5A059F1E349AF7E114	D43AF9B35473755C9684FC06D7D8CB70EE5C28E773FB294EB41EE71722924D24	UCA Extended Validation Root
8	SHECA RSA Extended Validation Server CA	Signing Key	sha256RSA	2048 bits	CN = SHECA RSA Extended Validation Server CA O = UniTrust C = CN	3B4B252A77372AFCB97FEDA8BDAF2299FC5DC5F4	4FD6FA527157EEA463689D7A4C2B934EF222279725413893D9847242C85CA9DF	UCA Extended Validation Root
9	SHECA EV Server CA G3	Signing Key	sha256RSA	2048 bits	CN = SHECA EV Server CA G3 O = UniTrust C = CN	54E972FB78669FE5CBF33B8F9846555373 9C0B84	7EF3F89456CE636557B20C5DFB37F98C253A0B660D2E9E5E7845CAF9C038C7C1	UCA Extended Validation Root

pwc

羅兵咸永道

#	Key Name	Key Type	Signature Algorithm	Key Size	Subject DN	Subject Key Identifier	Certificates Thumbprint (SHA256)	Certificate Signed by
10	SHECA Extended Validation SSL CA	Signing Key	sha256RSA	2048 bits	CN = SHECA Extended Validation SSL CA O = UniTrust C = CN	4D140DEA6B559C0CA6E1BB7BE86A966D175E7CB5	25BFDB1C5FE2CCE051EC6DFBF2BB24E78C92F969B1BB37867DAEDF93D1A7AE7E	UCA Extended Validation Root
11	UniTrust Global Root CA R1	Root Key	sha384RSA	4096 bits	CN = UniTrust Global Root CA R1 O = UniTrust C = CN	3CA061B0EFDAC6E8BB2DE156A2EBBBB63D232381	81B35EFC42C77947209D76B51B5E7B122CE78348AE8C4525DC8D4B30289E5385	UniTrust Global Root CA R1
12	SHECA EV Server CA 1A	Signing Key	sha384RSA	4096 bits	CN = SHECA EV Server CA 1A O = UniTrust C = CN	73E36DF62D862F57DF69A53687231C85E0170216	2F1CA1A5C0D7AE58C7ADFC69D4C57EE815F39C0F3D1F982E3AC76D25AB723995	UniTrust Global Root CA R1
13	UniTrust Global Root CA R2	Root Key	sha384ECDSA	384 bits	CN = UniTrust Global Root CA R2 O = UniTrust C = CN	E45366B7B7A4E9D7CCC121E04ACFCCAC01BC72BC	78919B35D1C615595A51328A5C546083B4D5320724A258695B991F2F61C4DCC7	UniTrust Global Root CA R2
14	SHECA EV Server CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA EV Server CA 2A O = UniTrust C = CN	44661C71EF69B7930AB5B771D83B114CFA843D77	93E49170D20F54DA701118A5ABDCDDA4FFCF334CDB2D8D80599AB62848C85F80	UniTrust Global Root CA R2
15	UniTrust Global TLS ECC Root CA R2	Root Key	sha384ECDSA	384 bits	CN = UniTrust Global TLS ECC Root CA R2 O = UniTrust C = CN	7935AD798A95305C3E05A675161A97000F6FCC90	6C689FC6B014A1FB0CDEB5A3996171C15E7286106028532E0210CEA8D9CD4E97	UniTrust Global TLS ECC Root CA R2
16	SHECA EV TLS ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA EV TLS ECC CA 2A O = UniTrust C = CN	B353900B5E40A4952EA85A27F413ABBAD631F233	05E4C4B1F258030690E6793C9C13C6F6AE234F68E5C41236FDC919B7F589032F	UniTrust Global TLS ECC Root CA R2
17	UniTrust Global TLS RSA Root CA R1	Root Key	sha384RSA	4096 bits	CN = UniTrust Global TLS RSA Root CA R1 O = UniTrust C = CN	F2ADBFAB6708F09672E633D65175A24759C900C4	4BABE0E9328D5DAE17936F3DDAA2442BFBDD0873F92FB8D1FBBD3D9894649AD9	UniTrust Global TLS RSA Root CA R1
18	SHECA EV TLS RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA EV TLS RSA CA 1A O = UniTrust C = CN	60651A135EAB2B98A5A1041B3057A1D02FC612E5	B2525A5966CA68CA7F504F0A21FD73847D174F89B48852A3E970588E1EAFC774	UniTrust Global TLS RSA Root CA R1

pwc

羅兵咸永道

Attachment B - Publicly disclosed incidents

Bugzilla ID	Disclosure	Publicly Disclosed Link
1735908	SHECA: UniTrust: Improper DER results in failure to comply with RFC 5280 - Encoded sequence component with default value	Bugzilla Ticket Link
1814288	SHECA: Delayed revocation of intermediate CA certificates	Bugzilla Ticket Link
1815527	SHECA: organizationName problems in OV and EV TLS certificates	Bugzilla Ticket Link
1787537	UniTrust: EV certificate with wildcard domain in common name and SAN	Bugzilla Ticket Link
1798626	SHECA: UniTrust: EV certificate with wrong Registry Country Name	Bugzilla Ticket Link
1838765	SHECA: Outdated Organizational Units (OUs) problems in OV TLS certificates	Bugzilla Ticket Link
1839105	SHECA: Non-compliant Subject Fields problem in OV TLS certificate	Bugzilla Ticket Link
1855997	SHECA: CRLs not downloading	Bugzilla Ticket Link
1856503	SHECA: Failure to revoke within 5 days	Bugzilla Ticket Link
1859694	SHECA: Issuance of test certificates	Bugzilla Ticket Link

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（简称“SHECA”）管理层

范围

我们接受委托，对后附 SHECA 于 2023 年 4 月 1 日至 2024 年 3 月 31 日期间于中国上海（包括设施 1 和设施 2）运营的 SSL 增强验证电子认证服务管理层认定执行了合理保证的鉴证业务。对于附录中所包括的根证书和中级证书，SHECA：

- 披露 SSL 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 v1.5.5;
  - UniTrust EV 证书电子认证业务规则 v1.5.4;
  - UniTrust EV 证书电子认证业务规则 v1.5.3;
  - UniTrust EV 证书电子认证业务规则 v1.5.2;
  - UniTrust EV 证书策略 v1.7.1;
  - UniTrust EV 证书策略 v1.7.0;
  - UniTrust EV 证书策略 v1.6.9; 以及
  - UniTrust EV 证书策略 v1.6.8,

  包括承诺遵循CAB论坛（CA/Browser Forum）的相关指引提供SSL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SSL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）SSL增强验证证书申请者的信息。

以符合 WebTrust 电子认证 SSL 增强验证审计标准 v1.8.

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 - SSL增强验证审计标准v1.8的规定。

我们的独立性和质量管理

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管理准则第 1 号，该准则要求事务所设计、实施并执行质量管理体系，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政策或程序。

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 - SSL 增强验证审计标准 v1.8 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 SSL 增强验证证书生命周期管理，包括 SSL 增强验证证书发放、更新和吊销的相关控制；（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。

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

由于内部控制体系本身的限制，SHECA 满足上述要求的能力可能会受到影响，例如：控制可能未达到预防、发现或纠正错误、舞弊、对系统或信息的未授权访问，或违反内外部制度或规定的要求。此外，风险的变化可能会影响本评估报告在将来时间的参考价值。

意见

我们认为，SHECA 于 2023 年 4 月 1 日至 2024 年 3 月 31 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 - SSL 增强验证审计标准 v1.8。

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 - SSL 增强验证审计标准 v1.8 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

UniTrust Global Root CA R1（附录 A#11），UniTrust Global Root CA R2（附录 A#13）在 2023 年 4 月 1 日至 2024 年 3 月 31 日期间未颁发证书，仅保持在线以提供吊销状态信息。

在 2023 年 4 月 1 日至 2024 年 3 月 31 日期间，SHECA 管理层披露了 10 起事件（见附录 B）。SHECA 所采取的补救措施和这些事件的根本原因已在 Bugzilla 网站的在线论坛以及组成 CA/Browser 论坛的各个互联网浏览器的在线论坛上公开发布。

目的及使用和分发限制

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 - SSL 增强验证审计标准 v1.8，因此后附 SHECA 管理层认定可能不适用于其他目的。本报告仅向 SHECA 管理层出具，用作向 WebTrust 电子认证 - SSL 增强验证审计标准 v1.8 相关机构提交报告后，在 SHECA 网站上获取并展示 WebTrust Seal，不应向任何其它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士负上或承担任何责任。

WebTrust seal 的使用

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。

罗兵咸永道会计师事务所
注册会计师

香港，2024年5月24日

[1] *SHECA 网站维护和网站的真实完整是公司管理层的职责。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。*

pwc

羅兵咸永道

附录 A

下表列示本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	主体识别名	密钥 ID	证书指纹（SHA256）	证书签发者
1	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	9BEA11C976FE014764C1BE56A6F914B5A5600317ABD9988393382E5161AA0493C	UCA Global G2 Root
2	SHECA EV Server CA G2	Signing Key	sha256RSA	2048 bits	CN = SHECA EV Server CA G2 O = UniTrust C = CN	86B148C0420A9C6F81FC4FDCD10F184BAAB5A6EA	4216527163AD2CAA825D3BF48F61A7661D0ABC89B58AB76B23A1E10999F0769F	UCA Global G2 Root
3	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	C1AFC65B1E813B0E6146E6AA5341681272ABE9A38D59F7BD1B27B729834A0D9C	Certum Trusted Network CA
4	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	3DD69C5BE170F943F804D1D31FE8F916C0C0226CDDD7AEA9AA9A0CDFD3474361	Certum Trusted Network CA
5	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	BB61408AED9F530B2EC0545E53BA2C8EBEAA57D9976447DB1663CED4600CD6B7	Certum Trusted Network CA
6	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	BFA95C5DF164B659FA32F6D10564D7170DDE661A853A782E6AB63639433BCB41	Certum Trusted Network CA
7	UCA Extended Validation Root	Root Key	sha256RSA	4096 bits	CN = UCA Extended Validation Root O = UniTrust C = CN	D9743AE4303D0DF712DC7E5A059F1E349AF7E114	D43AF9B35473755C9684FC06D7D8CB70EE5C28E773FB294EB41EE71722924D24	UCA Extended Validation Root
8	SHECA RSA Extended Validation Server CA	Signing Key	sha256RSA	2048 bits	CN = SHECA RSA Extended Validation Server CA O = UniTrust C = CN	3B4B252A77372AFCB97FEDA8BDAF2299FC5DC5F4	4FD6FA527157EEA463689D7A4C2B934EF222279725413893D9847242C85CA9DF	UCA Extended Validation Root
9	SHECA EV Server CA G3	Signing Key	sha256RSA	2048 bits	CN = SHECA EV Server CA G3 O = UniTrust C = CN	54E972FB78669FE5CBF33B8F98465553739C0B84	7EF3F89456CE636557B20C5DFB37F98C253A0B660D2E9E5E7845CAF9C038C7C1	UCA Extended Validation Root
10	SHECA Extended Validation SSL CA	Signing Key	sha256RSA	2048 bits	CN = SHECA Extended Validation SSL CA O = UniTrust C = CN	4D140DEA6B559C0CA6E1BB7BE86A966D175E7CB5	25BFDB1C5FE2CCE051EC6DFBF2BB24E78C92F969B1BB37867DAEDF93D1A7AE7E	UCA Extended Validation Root

pwc

羅兵咸永道

#	密钥名称	密钥种类	密钥算法	密钥长度	主体识别名	密钥 ID	证书指纹（SHA256）	证书签发者
11	UniTrust Global Root CA R1	Root Key	sha384RSA	4096 bits	CN = UniTrust Global Root CA R1 O = UniTrust C = CN	3CA061B0E FDAC6E8BB 2DE156A2E BBBB63D23 2381	81B35EFC42C7794720 9D76B51B5E7B122CE 78348AE8C4525DC8D 4B30289E5385	UniTrust Global Root CA R1
12	SHECA EV Server CA 1A	Signing Key	sha384RSA	4096 bits	CN = SHECA EV Server CA 1A O = UniTrust C = CN	73E36DF62 D862F57DF 69A5368723 1C85E01702 16	2F1CA1A5C0D7AE58C 7ADFC69D4C57EE815 F39C0F3D1F982E3AC 76D25AB723995	UniTrust Global Root CA R1
13	UniTrust Global Root CA R2	Root Key	sha384ECD SA	384 bits	CN = UniTrust Global Root CA R2 O = UniTrust C = CN	E45366B7B7 A4E9D7CCC 121E04ACFC CAC01BC72 BC	78919B35D1C615595A 51328A5C546083B4D 5320724A258695B991 F2F61C4DCC7	UniTrust Global Root CA R2
14	SHECA EV Server CA 2A	Signing Key	sha384ECD SA	384 bits	CN = SHECA EV Server CA 2A O = UniTrust C = CN	44661C71EF 69B7930AB 5B771D83B1 14CFA843D 77	93E49170D20F54DA7 01118A5ABDCDDA4F FCF334CDB2D8D805 99AB62848C85F80	UniTrust Global Root CA R2
15	UniTrust Global TLS ECC Root CA R2	Root Key	sha384ECD SA	384 bits	CN = UniTrust Global TLS ECC Root CA R2 O = UniTrust C = CN	7935AD798 A95305C3E 05A675161A 97000F6FC C90	6C689FC6B014A1FB0 CDEB5A3996171C15E7 2861060285 32E0210C EA8D9CD4E97	UniTrust Global TLS ECC Root CA R2
16	SHECA EV TLS ECC CA 2A	Signing Key	sha384ECD SA	384 bits	CN = SHECA EV TLS ECC CA 2A O = UniTrust C = CN	B353900B5 E40A4952E A85A27F413 ABBAD631F 233	05E4C4B1F25803069 0E6793C9C13C6F6AE 234F68E5C41236FDC 919B7F589032F	UniTrust Global TLS ECC Root CA R2
17	UniTrust Global TLS RSA Root CA R1	Root Key	sha384RSA	4096 bits	CN = UniTrust Global TLS RSA Root CA R1 O = UniTrust C = CN	F2ADBFAB6 708F09672E 633D65175A 24759C900C 4	4BABE0E9328D5DAE 17936F3DDAA2442BF BDD0873F92FB8D1F BBD3D9894649AD9	UniTrust Global TLS RSA Root CA R1
18	SHECA EV TLS RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA EV TLS RSA CA 1A O = UniTrust C = CN	60651A135E AB2B98A5A 1041B3057A 1D02FC612E 5	B2525A5966CA68CA7 F504F0A21FD73847D 174F89B48852A3E97 0588E1EAFC774	UniTrust Global TLS RSA Root CA R1

pwc

羅兵咸永道

附录 B – 公开披露的事件

Bugzilla ID	**披露**	**公开披露的链接**
1735908	SHECA: UniTrust: Improper DER results in failure to comply with RFC 5280 - Encoded sequence component with default value	Bugzilla Ticket Link
1814288	SHECA: Delayed revocation of intermediate CA certificates	Bugzilla Ticket Link
1815527	SHECA: organizationName problems in OV and EV TLS certificates	Bugzilla Ticket Link
1787537	UniTrust: EV certificate with wildcard domain in common name and SAN	Bugzilla Ticket Link
1798626	SHECA: UniTrust: EV certificate with wrong Registry Country Name	Bugzilla Ticket Link
1838765	SHECA: Outdated Organizational Units (OUs) problems in OV TLS certificates	Bugzilla Ticket Link
1839105	SHECA: Non-compliant Subject Fields problem in OV TLS certificate	Bugzilla Ticket Link
1855997	SHECA: CRLs not downloading	Bugzilla Ticket Link
1856503	SHECA: Failure to revoke within 5 days	Bugzilla Ticket Link
1859694	SHECA: Issuance of test certificates	Bugzilla Ticket Link

Shanghai Electronic Certificate Authority Co.,Ltd

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

PricewaterhouseCoopers
22/F, Prince's Building, Central, Hong Kong

May 24, 2024

Dear Sirs,

Assertion of Management as to the Disclosure to Business Practices and Controls over the Certification Authority - Extended Validation SSL Operations during the period from April 1, 2023 through March 31, 2024

Shanghai Electronic Certificate Authority 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 SSL ("EV SSL") CA services.

The management of SHECA is responsible for establishing and maintaining effective controls over its EV SSL CA operations, including its EV SSL CA business practices disclosure on its website, EV SSL key lifecycle management controls, and EV SSL 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 SSL CA services. Based on that assessment, in SHECA management's opinion, in providing its EV SSL Certification Authority (CA) services at Shanghai (including Facility 1 and Facility 2), China, throughout the period April 1, 2023 to March 31, 2024, SHECA has:

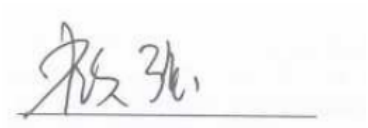
- disclosed its extended validation SSL ("EV SSL") certificate lifecycle management business practices in its:
  - UniTrust EV Certification Practice Statement v1.5.5;
  - UniTrust EV Certification Practice Statement v1.5.4;
  - UniTrust EV Certification Practice Statement v1.5.3;
  - UniTrust EV Certification Practice Statement v1.5.2;
  - UniTrust EV Certificate Policy Version 1.7.1;
  - UniTrust EV Certificate Policy Version 1.7.0;
  - UniTrust EV Certificate Policy Version 1.6.9; and
  - UniTrust EV Certificate Policy Version 1.6.8,

including its commitment to provide EV SSL 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 SSL certificates it manages is established and protected throughout their lifecycles; and
  - EV SSL subscriber information is properly authenticated (for the registration activities performed by SHECA),

in accordance with the WebTrust Principles and Criteria for Certification Authorities - Extended Validation SSL v1.8.

The UniTrust Global Root CA R1 (Appendix #11), UniTrust Global Root CA R2 (Appendix #13) CAs did not issue certificates during the period April 1, 2023 to March 31, 2024 and were maintained online to provide revocation status information only.



Mr. Cui Jiuqiang
General Manager of Shanghai Electronic Certificate Authority 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 DN	Subject Key Identifier	Certificates Thumbprint (SHA256)	Certificate Signed by
1	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	9BEA11C976FE014764C1BE56A6F914B5A5603017ABD9988393382E5161AA0493C	UCA Global G2 Root
2	SHECA EV Server CA G2	Signing Key	sha256RSA	2048 bits	CN = SHECA EV Server CA G2 O = UniTrust C = CN	86B148C0420A9C6F81FC4FDCD10F184BAAB5A6EA	4216527163AD2CAA825D3BF48F61A7661D0ABC89B58AB76B23A1E10999F0769F	UCA Global G2 Root
3	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	C1AFC65B1E813B0E6146E6AA5341681272ABE9A38D59F7BD1B27B729834A0D9C	Certum Trusted Network CA
4	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	3DD69C5BE170F943F804D1D31FE8F916C0C0226CDDD7AEA9AA9A0CDFD3474361	Certum Trusted Network CA
5	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	BB61408AED9F530B2EC0545E53BA2C8EBEAA57D9976447DB1663CED4600CD6B7	Certum Trusted Network CA
6	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	BFA95C5DF164B659FA32F6D10564D7170DDE661A853A782E6AB63639433BCB41	Certum Trusted Network CA
7	UCA Extended Validation Root	Root Key	sha256RSA	4096 bits	CN = UCA Extended Validation Root O = UniTrust C = CN	D9743AE4303D0DF712DC7E5A059F1E349AF7E114	D43AF9B35473755C9684FC06D7D8CB70EE5C28E773FB294EB41EE71722924D24	UCA Extended Validation Root
8	SHECA RSA Extended Validation Server CA	Signing Key	sha256RSA	2048 bits	CN = SHECA RSA Extended Validation Server CA O = UniTrust C = CN	3B4B252A77372AFCB97FEDA8BDAF2299FC5DC5F4	4FD6FA527157EEA463689D7A4C2B934EF222279725413893D9847242C85CA9DF	UCA Extended Validation Root
9	SHECA EV Server CA G3	Signing Key	sha256RSA	2048 bits	CN = SHECA EV Server CA G3 O = UniTrust C = CN	54E972FB78669FE5CBF33B8F98465553739C0B84	7EF3F89456CE636557B20C5DFB37F98C253A0B660D2E9E5E7845CAF9C038C7C1	UCA Extended Validation Root
10	SHECA Extended Validation SSL CA	Signing Key	sha256RSA	2048 bits	CN = SHECA Extended Validation SSL CA O = UniTrust C = CN	4D140DEA6B559C0CA6E1BB7BE86A966D175E7CB5	25BFDB1C5FE2CCE051EC6DFBF2BB24E78C92F969B1BB37867DAEDF93D1A7AE7E	UCA Extended Validation Root
11	UniTrust Global Root CA R1	Root Key	sha384RSA	4096 bits	CN = UniTrust Global Root CA R1 O = UniTrust C = CN	3CA061B0EFDAC6E8BB2DE156A2EBBBB63D232381	81B35EFC42C77947209D76B51B5E7B122CE78348AE8C4525DC8D4B30289E5385	UniTrust Global Root CA R1

#	Key Name	Key Type	Signature Algorithm	Key Size	Subject DN	Subject Key Identifier	Certificates Thumbprint (SHA256)	Certificate Signed by
12	SHECA EV Server CA 1A	Signing Key	sha384RSA	4096 bits	CN = SHECA EV Server CA 1A O = UniTrust C = CN	73E36DF62D862F57DF69A53687231C85E0170216	2F1CA1A5C0D7AE58C7ADFC69D4C57EE815F39C0F3D1F982E3AC76D25AB723995	UniTrust Global Root CA R1
13	UniTrust Global Root CA R2	Root Key	sha384ECDSA	384 bits	CN = UniTrust Global Root CA R2 O = UniTrust C = CN	E45366B7B7A4E9D7CCC121E04ACFCCAC01BC72BC	78919B35D1C615595A51328A5C546083B4D5320724A258695B991F2F61C4DCC7	UniTrust Global Root CA R2
14	SHECA EV Server CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA EV Server CA 2A O = UniTrust C = CN	44661C71EF69B7930AB5B771D83B114CFA843D77	93E49170D20F54DA701118A5ABDCDDA4FFCF334CDB2D8D80599AB62848C85F80	UniTrust Global Root CA R2
15	UniTrust Global TLS ECC Root CA R2	Root Key	sha384ECDSA	384 bits	CN = UniTrust Global TLS ECC Root CA R2 O = UniTrust C = CN	7935AD798A95305C3E05A675161A97000F6FCC90	6C689FC6B014A1FB0CDEB5A3996171C15E72861060285320E0210CEA8D9CD4E97	UniTrust Global TLS ECC Root CA R2
16	SHECA EV TLS ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA EV TLS ECC CA 2A O = UniTrust C = CN	B353900B5E40A4952EA85A27F413ABBAD631F233	05E4C4B1F258030690E6793C9C13C6F6AE234F68E5C41236FDC919B7F589032F	UniTrust Global TLS ECC Root CA R2
17	UniTrust Global TLS RSA Root CA R1	Root Key	sha384RSA	4096 bits	CN = UniTrust Global TLS RSA Root CA R1 O = UniTrust C = CN	F2ADBFAB6708F09672E633D65175A24759C900C4	4BABE0E9328D5DAE17936F3DDAA2442BFBDD0873F92FB8D1FBBD3D9894649AD9	UniTrust Global TLS RSA Root CA R1
18	SHECA EV TLS RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA EV TLS RSA CA 1A O = UniTrust C = CN	60651A135EAB2B98A5A1041B3057A1D02FC612E5	B2525A5966CA68CA7F504F0A21FD73847D174F89B48852A3E970588E1EAFC774	UniTrust Global TLS RSA Root CA R1

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
香港中环太子大厦22楼

2024 年 5 月 24 日

致：罗兵咸永道会计师事务所

就 2023 年 4 月 1 日到 2024 年 3 月 31 日期间 SSL 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 Co., Ltd.，简称“SHECA”）运营电子认证服务机构，并提供 SSL 增强验证电子认证服务，附录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 SSL 增强验证服务建立并维护有效的控制，包括：披露 SSL 增强验证业务规则，SSL 增强验证密钥生命周期管理，以及 SSL 增强验证证书生命周期管理。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 SSL 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 2023 年 4 月 1 日至 2024 年 3 月 31 日就 SHECA 在中国上海（包括设施 1 和设施 2）所提供的 SSL 增强验证电子认证服务期间，SHECA：

- 披露SSL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 v1.5.5;
  - UniTrust EV 证书电子认证业务规则 v1.5.4;
  - UniTrust EV 证书电子认证业务规则 v1.5.3;
  - UniTrust EV 证书电子认证业务规则 v1.5.2;
  - UniTrust EV 证书策略 1.7.1;
  - UniTrust EV 证书策略 1.7.0;
  - UniTrust EV 证书策略 1.6.9; 以及
  - UniTrust EV 证书策略 1.6.8,

包括承诺遵循CAB论坛（CA/Browser Forum）的相关指引提供SSL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SSL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）SSL增强验证证书申请者的信息。

以符合 WebTrust电子认证SSL增强验证审计标准 v1.8.

UniTrust Global Root CA R1（附录#11），UniTrust Global Root CA R2（附录#13）在 2023 年 4 月 1 日至 2024 年 3 月 31 日期间未颁发证书，仅保持在线以提供吊销状态信息。

_____

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

附录

下表列示本管理层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	主体识别名	密钥 ID	证书指纹（SHA256）	证书签发者
1	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	9BEA11C976FE014764C1BE56A6F914B5A5600317ABD99883933825161AA0493C	UCA Global G2 Root
2	SHECA EV Server CA G2	Signing Key	sha256RSA	2048 bits	CN = SHECA EV Server CA G2 O = UniTrust C = CN	86B148C0420A9C6F81FC4FDCD10F184BAAB5A6EA	4216527163AD2CAA825D3BF48F61A7661D0ABC89B58AB76B23A1E10999F0769F	UCA Global G2 Root
3	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	C1AFC65B1E813B0E6146E6AA5341681272ABE9A38D59F7BD1B27B729834A0D9C	Certum Trusted Network CA
4	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	3DD69C5BE170F943F804D1D31FE8F916C0C0226CDDD7AEA9AA9A0CDFD3474361	Certum Trusted Network CA
5	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	BB61408AED9F530B2EC0545E53BA2C8EBEAA57D9976447DB1663CED4600CD6B7	Certum Trusted Network CA
6	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	BFA95C5DF164B659FA32F6D10564D7170DDE661A853A782E6AB63639433BCB41	Certum Trusted Network CA
7	UCA Extended Validation Root	Root Key	sha256RSA	4096 bits	CN = UCA Extended Validation Root O = UniTrust C = CN	D9743AE4303D0DF712DC7E5A059F1E349AF7E114	D43AF9B35473755C9684FC06D7D8CB70EE5C28E773FB294EB41EE71722924D24	UCA Extended Validation Root
8	SHECA RSA Extended Validation Server CA	Signing Key	sha256RSA	2048 bits	CN = SHECA RSA Extended Validation Server CA O = UniTrust C = CN	3B4B252A77372AFCB97FEDA8BDAF2299FC5DC5F4	4FD6FA527157EEA463689D7A4C2B934EF222279725413893D9847242C85CA9DF	UCA Extended Validation Root
9	SHECA EV Server CA G3	Signing Key	sha256RSA	2048 bits	CN = SHECA EV Server CA G3 O = UniTrust C = CN	54E972FB78669FE5CBF33B8F98465553739C0B84	7EF3F89456CE636557B20C5DFB37F98C253A0B660D2E9E5E7845CAF9C038C7C1	UCA Extended Validation Root
10	SHECA Extended Validation SSL CA	Signing Key	sha256RSA	2048 bits	CN = SHECA Extended Validation SSL CA O = UniTrust C = CN	4D140DEA6B559C0CA6E1BB7BE86A966D175E7CB5	25BFDB1C5FE2CCE051EC6DFBF2BB24E78C92F969B1BB37867DAEDF93D1A7AE7E	UCA Extended Validation Root
11	UniTrust Global Root CA R1	Root Key	sha384RSA	4096 bits	CN = UniTrust Global Root CA R1 O = UniTrust C = CN	3CA061B0EFDAC6E8BB2DE156A2EBBBB63D232381	81B35EFC42C77947209D76B51B5E7B122CE78348AE8C4525DC8D4B30289E5385	UniTrust Global Root CA R1

#	密钥名称	密钥种类	密钥算法	密钥长度	主体识别名	密钥 ID	证书指纹（SHA256）	证书签发者
12	SHECA EV Server CA 1A	Signing Key	sha384RSA	4096 bits	CN = SHECA EV Server CA 1A O = UniTrust C = CN	73E36DF62D862F57DF69A53687231C85E0170216	2F1CA1A5C0D7AE58C7ADFC69D4C57EE815F39C0F3D1F982E3AC76D25AB723995	UniTrust Global Root CA R1
13	UniTrust Global Root CA R2	Root Key	sha384ECDSA	384 bits	CN = UniTrust Global Root CA R2 O = UniTrust C = CN	E45366B7B7A4E9D7CCC121E04ACFCCAC01BC72BC	78919B35D1C615595A51328A5C546083B4D5320724A258695B991F2F61C4DCC7	UniTrust Global Root CA R2
14	SHECA EV Server CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA EV Server CA 2A O = UniTrust C = CN	44661C71EF69B7930AB5B771D83B114CFA843D77	93E49170D20F54DA701118A5ABDCDDA4FFCF334CDB2D8D80599AB62848C85F80	UniTrust Global Root CA R2
15	UniTrust Global TLS ECC Root CA R2	Root Key	sha384ECDSA	384 bits	CN = UniTrust Global TLS ECC Root CA R2 O = UniTrust C = CN	7935AD798A95305C3E05A675161A97000F6FCC90	6C689FC6B014A1FB0CDEB5A3996171C15E7286106028532E0210CEA8D9CD4E97	UniTrust Global TLS ECC Root CA R2
16	SHECA EV TLS ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA EV TLS ECC CA 2A O = UniTrust C = CN	B353900B5E40A4952EA85A27F413ABBAD631F233	05E4C4B1F258030690E6793C9C13C6F6AE234F68E5C41236FDC919B7F589032F	UniTrust Global TLS ECC Root CA R2
17	UniTrust Global TLS RSA Root CA R1	Root Key	sha384RSA	4096 bits	CN = UniTrust Global TLS RSA Root CA R1 O = UniTrust C = CN	F2ADBFAB6708F09672E633D65175A24759C900C4	4BABE0E9328D5DAE17936F3DDAA2442BFBDD0873F92FB8D1FBBD3D9894649AD9	UniTrust Global TLS RSA Root CA R1
18	SHECA EV TLS RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA EV TLS RSA CA 1A O = UniTrust C = CN	60651A135EAB2B98A5A1041B3057A1D02FC612E5	B2525A5966CA68CA7F504F0A21FD73847D174F89B48852A3E970588E1EAFC774	UniTrust Global TLS RSA Root CA R1