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 September 1, 2023 to March 31, 2024, for its CAs enumerated in the Attachment A, SHECA has:

- disclosed its S/MIME certificate lifecycle management business practices in its:
  - UniTrust Certification Practice Statement v3.7.7;
  - UniTrust Certification Practice Statement v3.7.6;
  - UniTrust Certificate Policy v1.5.5;
  - UniTrust Certificate Policy v1.5.4; and
  - UniTrust Certificate Policy v1.5.3,

  including its commitment to provide S/MIME certificates in conformity with the CA/Browser Forum Requirements 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 S/MIME certificates it manages is established and protected throughout their lifecycles; and
  - S/MIME subscriber information is properly authenticated (for the registration activities performed by SHECA),

- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorized individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity,

in accordance with the WebTrust Principles and Criteria for Certification Authorities – S/MIME Certificates v1.0.1.

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 – S/MIME Certificates v1.0.1.

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 - S/MIME Certificates v1.0.1. 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) obtaining an understanding of SHECA’s S/MIME certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of S/MIME certificates; (2) selectively testing transactions executed in accordance with disclosed S/MIME certificate lifecycle management business 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.

Opinion

In our opinion, the management's assertion of SHECA, for the period from September 1, 2023 to March 31, 2024, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities - S/MIME Certificates v1.0.1.

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 - S/MIME Certificates v1.0.1, nor the suitability of any of SHECA's services for any customer's intended purpose.

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 - S/MIME Certificates v1.0.1 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 - S/MIME Certificates v1.0.1.

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.

[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.

Use of the WebTrust seal

SHECA’s use of the WebTrust for Certification Authorities - S/MIME Certificates 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

PricewaterhouseCoopers
Certified Public Accountants

Hong Kong, 24 May 2024

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	9BEA11C976FE014764C1BE56A6F914B5A560317ABD9988393382E5161AA0493C	UCA Global G2 Root
2	SHECA SMIME CA G1	Signing Key	sha256RSA	2048 bits	CN = SHECA SMIME CA G1 O = UniTrust C = CN	1FA80B4DCF9CA6A53ADAB096AB9957B90A9B7F5D	8100D384D6C4529883C37C37C68FD4903C41CCBCB9033A9C733A6AF0806E1DE7	UCA Global G2 Root
3	UniTrust Global SMIME ECC Root CA R2	Root Key	sha384ECDSA	384 bits	CN = UniTrust Global SMIME ECC Root CA R2 O = UniTrust C = CN	2D4D94407CFFC45D4357F190557448CF6CBEA343	6F4E2464D216A1E0B558BB204259B4A545AEB948957AA3EAF11B2F4DE1AFEF10	UniTrust Global SMIME ECC Root CA R2
4	SHECA IV SMIME ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA IV SMIME ECC CA 2A O = UniTrust C = CN	EBC1D6F67F2909A9928A90B4295818A02F3CAF1B	E82D794C1AC79F9BEBF3B6D98A237F84C15FD40C3ABB86C2214E699414F8FF54	UniTrust Global SMIME ECC Root CA R2
5	SHECA MV SMIME ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA MV SMIME ECC CA 2A O = UniTrust C = CN	FE0328035B693E5EDC5FAE0B742735DCC38C66F0	D7C4AB9D315AE8B889DA902C55264295D8CDC0F5471370490F4D4585E2C3C6D3	UniTrust Global SMIME ECC Root CA R2
6	SHECA OV SMIME ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA OV SMIME ECC CA 2A O = UniTrust C = CN	BD34144476B06D0F264C3CA9C349AC7153D4EF55	229B7FBCA2361DE63171067DE91DFFB3D2FA71A5ABE51CA41D5300C5750D2F0E	UniTrust Global SMIME ECC Root CA R2
7	UniTrust Global SMIME RSA Root CA R1	Root Key	sha384RSA	4096 bits	CN = UniTrust Global SMIME RSA Root CA R1 O = UniTrust C = CN	DF08E3E977C1F0FBF5F8D419504C7719F206CBA3	F0F255ADA2A643C0A1E7C8F54F3ED3DD25EF0E7378E76F7C127517ECFD952803	UniTrust Global SMIME RSA Root CA R1
8	SHECA IV SMIME RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA IV SMIME RSA CA 1A O = UniTrust C = CN	D38BCDC445B1E8D0AFDD8BE8E4A6B5B30A71EF4E	82BA6F1067468383757DF53F1628258043BBB972E1CAD31FD7AAD0ADD66A5B53	UniTrust Global SMIME RSA Root CA R1
9	SHECA MV SMIME RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA MV SMIME RSA CA 1A O = UniTrust C = CN	5A4AEFED9AE84052DA320BBB32C4E529ECDC5255	92148A115D26B287254B36164164B2220EE36B405D3B708CF5B7AB060C66B1FE	UniTrust Global SMIME RSA Root CA R1

#	Key Name	Key Type	Signature Algorithm	Key Size	Subject DN	Subject Key Identifier	Certificates Thumbprint (SHA256)	Certificate Signed by
10	SHECA OV SMIME RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA OV SMIME RSA CA 1A O = UniTrust C = CN	C061C3D053C9F412C5C9192DBB638305E4CA7EF8	6B661B964F2359C4CA68355243A2EEEDA9BACDA191D103A0C1119EC892018AC7	UniTrust Global SMIME RSA Root CA R1

pwc 羅兵咸永道

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9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S/MIME邮件安全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A中所包括的根证书和中级证书，SHECA:

- 披露邮件安全证书生命周期管理业务规则于:
  - UniTrust证书认证业务规则 v3.7.7;
  - UniTrust证书认证业务规则 v3.7.6;
  - UniTrust证书策略 v1.5.5;
  - UniTrust证书策略 v1.5.4; 以及
  - UniTrust证书策略 v1.5.3,

包括承诺遵循CAB论坛（CA/Browser Forum）的相关指引提供邮件安全服务，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:
  - 有效维护密钥与邮件安全证书在生命周期中的完整性；
  - 恰当地鉴定（SHECA所执行的注册操作）邮件安全证书申请者的信息，

- 通过有效控制机制，以提供以下合理保证:
  - 对CA系统和数据的逻辑和物理访问仅限于授权的个人；
  - 保持密钥和证书管理操作的连续性；以及
  - CA 系统的开发、维护和操作得到适当授权和执行，以保持 CA 系统的完整性，

以符合 WebTrust 电子认证邮件安全基准规范审计标准 v1.0.1.

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 – 邮件安全基准规范审计标准v1.0.1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 – 邮件安全基准规范审计标准 v1.01 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 邮件安全证书生命周期管理业务实践，包括邮件安全证书发放、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 9 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 – 邮件安全基准规范审计标准 v1.0.1。

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 – 邮件安全基准规范审计标准 v1.0.1 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。

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 – 邮件安全基准规范审计标准 v1.0.1，因此后附 SHECA 管理层认定可能不适用于其他目的。本报告仅向 SHECA 管理层出具，用作向 WebTrust 电子认证 - 邮件安全基准规范审计标准 v1.0.1 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。*

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	9BEA11C976FE014764C1BE56A6F914B5A560317ABD9988393382E5161AA0493C	UCA Global G2 Root
2	SHECA SMIME CA G1	Signing Key	sha256RSA	2048 bits	CN = SHECA SMIME CA G1 O = UniTrust C = CN	1FA80B4DCF9CA6A53ADAB096AB9957B90A9B7F5D	8100D384D6C4529883C37C37C68FD4903C41CCBCB9033A9C733A6AF0806E1DE7	UCA Global G2 Root
3	UniTrust Global SMIME ECC Root CA R2	Root Key	sha384ECDSA	384 bits	CN = UniTrust Global SMIME ECC Root CA R2 O = UniTrust C = CN	2D4D94407CFFC45D4357F190557448CF6CBEA343	6F4E2464D216A1E0B558BB204259B4A545AEB948957AA3EAF11B2F4DE1AFEF10	UniTrust Global SMIME ECC Root CA R2
4	SHECA IV SMIME ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA IV SMIME ECC CA 2A O = UniTrust C = CN	EBC1D6F67F2909A9928A90B4295818A02F3CAF1B	E82D794C1AC79F9BEBF3B6D98A237F84C15FD40C3ABB86C2214E699414F8FF54	UniTrust Global SMIME ECC Root CA R2
5	SHECA MV SMIME ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA MV SMIME ECC CA 2A O = UniTrust C = CN	FE0328035B693E5EDC5FAE0B742735DCC38C66F0	D7C4AB9D315AE8B889DA902C55264295D8CDC0F5471370490F4D4585E2C3C6D3	UniTrust Global SMIME ECC Root CA R2
6	SHECA OV SMIME ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA OV SMIME ECC CA 2A O = UniTrust C = CN	BD34144476B06D0F264C3CA9C349AC7153D4EF55	229B7FBCA2361DE63171067DE91DFFB3D2FA71A5ABE51CA41D5300C5750D2F0E	UniTrust Global SMIME ECC Root CA R2
7	UniTrust Global SMIME RSA Root CA R1	Root Key	sha384RSA	4096 bits	CN = UniTrust Global SMIME RSA Root CA R1 O = UniTrust C = CN	DF08E3E977C1F0FBF5F8D419504C7719F206CBA3	F0F255ADA2A643C0A1E7C8F54F3ED3DD25EF0E7378E76F7C127517ECFD952803	UniTrust Global SMIME RSA Root CA R1
8	SHECA IV SMIME RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA IV SMIME RSA CA 1A O = UniTrust C = CN	D38BCDC445B1E8D0AFDD8BE8E4A6B5B30A71EF4E	82BA6F1067468383757DF53F1628258043BBB972E1CAD31FD7AAD0ADD66A5B53	UniTrust Global SMIME RSA Root CA R1
9	SHECA MV SMIME RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA MV SMIME RSA CA 1A O = UniTrust C = CN	5A4AEFED9AE84052DA320BBB32C4E529ECDC5255	92148A115D26B287254B36164164B2220EE36B405D3B708CF5B7AB060C66B1FE	UniTrust Global SMIME RSA 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
10	SHECA OV SMIME RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA OV SMIME RSA CA 1A O = UniTrust C = CN	C061C3D053C9F412C5C9192DBB638305E4CA7EF8	6B661B964F2359C4CA68355243A2EEEDA9BACDA191D103A0C1119EC892018AC7	UniTrust Global SMIME RSA Root CA R1

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 of Business Practices and Controls over the Certification Authority – S/MIME Operations during the period from September 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) for S/MIME CA services.

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

- disclosed its S/MIME certificate lifecycle management business practices in its:
    - UniTrust Certification Practice Statement v3.7.7;
    - UniTrust Certification Practice Statement v3.7.6;
    - UniTrust Certificate Policy v1.5.5;
    - UniTrust Certificate Policy v1.5.4; and
    - UniTrust Certificate Policy v1.5.3,

  including its commitment to provide S/MIME certificates in conformity with the CA/Browser Forum Requirements 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 S/MIME certificates it manages is established and protected throughout their lifecycles; and
  - S/MIME subscriber information is properly authenticated (for the registration activities performed by SHECA),

- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorized individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity,

in accordance with the WebTrust Principles and Criteria for Certification Authorities – S/MIME Certificates v1.0.1.

Mr. Cui Jiuqiang
General Manager of Shanghai Electronic Certificate Authority 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'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	9BEA11C976FE014764C1BE56A6F914B5A560317ABD9988393382E5161AA0493C	UCA Global G2 Root
2	SHECA SMIME CA G1	Signing Key	sha256RSA	2048 bits	CN = SHECA SMIME CA G1 O = UniTrust C = CN	1FA80B4DCF9CA6A53ADAB096AB9957B90A9B7F5D	8100D384D6C4529883C37C37C68FD4903C41CCBCB9033A9C733A6AF0806E1DE7	UCA Global G2 Root
3	UniTrust Global SMIME ECC Root CA R2	Root Key	sha384ECDSA	384 bits	CN = UniTrust Global SMIME ECC Root CA R2 O = UniTrust C = CN	2D4D94407CFFC45D4357F190557448CF6CBEA343	6F4E2464D216A1E0B558BB204259B4A545AEB948957AA3EAF11B2F4DE1AFEF10	UniTrust Global SMIME ECC Root CA R2
4	SHECA IV SMIME ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA IV SMIME ECC CA 2A O = UniTrust C = CN	EBC1D6F67F2909A9928A90B4295818A02F3CAF1B	E82D794C1AC79F9BEBF3B6D98A237F84C15FD40C3ABB86C2214E699414F8FF54	UniTrust Global SMIME ECC Root CA R2
5	SHECA MV SMIME ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA MV SMIME ECC CA 2A O = UniTrust C = CN	FE0328035B693E5EDC5FAE0B742735DCC38C66F0	D7C4AB9D315AE8B889DA902C55264295D8CDC0F5471370490F4D4585E2C3C6D3	UniTrust Global SMIME ECC Root CA R2
6	SHECA OV SMIME ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA OV SMIME ECC CA 2A O = UniTrust C = CN	BD34144476B06D0F264C3CA9C349AC7153D4EF55	229B7FBCA2361DE63171067DE91DFFB3D2FA71A5ABE51CA41D5300C5750D2F0E	UniTrust Global SMIME ECC Root CA R2
7	UniTrust Global SMIME RSA Root CA R1	Root Key	sha384RSA	4096 bits	CN = UniTrust Global SMIME RSA Root CA R1 O = UniTrust C = CN	DF08E3E977C1F0FBF5F8D419504C7719F206CBA3	F0F255ADA2A643C0A1E7C8F54F3ED3DD25EF0E7378E76F7C127517ECFD952803	UniTrust Global SMIME RSA Root CA R1
8	SHECA IV SMIME RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA IV SMIME RSA CA 1A O = UniTrust C = CN	D38BCDC445B1E8D0AFDD8BE8E4A6B5B30A71EF4E	82BA6F1067468383757DF53F1628258043BBB972E1CAD31FD7AAD0ADD66A5B53	UniTrust Global SMIME RSA Root CA R1
9	SHECA MV SMIME RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA MV SMIME RSA CA 1A O = UniTrust C = CN	5A4AEFED9AE84052DA320BBB32C4E529ECDC5255	92148A115D26B287254B36164164B2220EE36B405D3B708CF5B7AB060C66B1FE	UniTrust Global SMIME RSA Root CA R1
10	SHECA OV SMIME RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA OV SMIME RSA CA 1A O = UniTrust C = CN	C061C3D053C9F412C5C9192DBB638305E4CA7EF8	6B661B964F2359C4CA68355243A2EEEDA9BACDA191D103A0C1119EC892018AC7	UniTrust Global SMIME 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 9 月 1 日到 2024 年 3 月 31 日期间邮件安全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，并提供邮件安全电子认证服务，附录列示了服务所包括的根证书和中级证书。

SHECA 的管理层负责针对邮件安全服务建立并维护有效的控制，包括：邮件安全签名业务规则，邮件安全密钥生命周期管理，邮件安全证书生命周期管理。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邮件安全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 9 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）提供的邮件安全电子认证服务期间，SHECA：

- 披露邮件安全证书生命周期管理业务规则于:
  - UniTrust证书认证业务规则 v3.7.7;
  - UniTrust证书认证业务规则 v3.7.6;
  - UniTrust证书策略 v1.5.5;
  - UniTrust证书策略 v1.5.4;以及
  - UniTrust证书策略 v1.5.3,

包括承诺遵循CAB论坛（CA/Browser Forum）的相关指引提供邮件安全服务，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：
  - 恰当地鉴定（SHECA所执行的注册操作）代码签名证书申请者的信息；以及

- 有效维护密钥与代码签名证书在生命周期中的完整性，

- 通过有效控制机制，以提供以下合理保证:
  - 对CA系统和数据的逻辑和物理访问仅限于授权的个人；
  - 保持密钥和证书管理操作的连续性；以及
  - CA 系统的开发、维护和操作得到适当授权和执行，以保持 CA 系统的完整性，

以符合 WebTrust 电子认证邮件安全基准规范审计标准 v1.0.1.

____

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	9BEA11C976FE014764C1BE56A6F914B5A560317ABD9988393382E5161AA0493C	UCA Global G2 Root
2	SHECA SMIME CA G1	Signing Key	sha256RSA	2048 bits	CN = SHECA SMIME CA G1 O = UniTrust C = CN	1FA80B4DCF9CA6A53ADAB096AB9957B90A9B7F5D	8100D384D6C4529883C37C37C68FD4903C41CCBCB9033A9C733A6AF0806E1DE7	UCA Global G2 Root
3	UniTrust Global SMIME ECC Root CA R2	Root Key	sha384ECDSA	384 bits	CN = UniTrust Global SMIME ECC Root CA R2 O = UniTrust C = CN	2D4D94407CFFC45D4357F190557448CF6CBEA343	6F4E2464D216A1E0B558BB204259B4A545AEB948957AA3EAF11B2F4DE1AFEF10	UniTrust Global SMIME ECC Root CA R2
4	SHECA IV SMIME ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA IV SMIME ECC CA 2A O = UniTrust C = CN	EBC1D6F67F2909A9928A90B4295818A02F3CAF1B	E82D794C1AC79F9BEBF3B6D98A237F84C15FD40C3ABB86C2214E699414F8FF54	UniTrust Global SMIME ECC Root CA R2
5	SHECA MV SMIME ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA MV SMIME ECC CA 2A O = UniTrust C = CN	FE0328035B693E5EDC5FAE0B742735DCC38C66F0	D7C4AB9D315AE8B889DA902C55264295D8CDC0F5471370490F4D4585E2C3C6D3	UniTrust Global SMIME ECC Root CA R2
6	SHECA OV SMIME ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA OV SMIME ECC CA 2A O = UniTrust C = CN	BD34144476B06D0F264C3CA9C349AC7153D4EF55	229B7FBCA2361DE63171067DE91DFFB3D2FA71A5ABE51CA41D5300C5750D2F0E	UniTrust Global SMIME ECC Root CA R2
7	UniTrust Global SMIME RSA Root CA R1	Root Key	sha384RSA	4096 bits	CN = UniTrust Global SMIME RSA Root CA R1 O = UniTrust C = CN	DF08E3E977C1F0FBF5F8D419504C7719F206CBA3	F0F255ADA2A643C0A1E7C8F54F3ED3DD25EF0E7378E76F7C127517ECFD952803	UniTrust Global SMIME RSA Root CA R1
8	SHECA IV SMIME RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA IV SMIME RSA CA 1A O = UniTrust C = CN	D38BCDC445B1E8D0AFDD8BE8E4A6B5B30A71EF4E	82BA6F1067468383757DF53F1628258043BBB972E1CAD31FD7AAD0ADD66A5B53	UniTrust Global SMIME RSA Root CA R1
9	SHECA MV SMIME RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA MV SMIME RSA CA 1A O = UniTrust C = CN	5A4AEFED9AE84052DA320BBB32C4E529ECDC5255	92148A115D26B287254B36164164B2220EE36B405D3B708CF5B7AB060C66B1FE	UniTrust Global SMIME RSA Root CA R1
10	SHECA OV SMIME RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA OV SMIME RSA CA 1A O = UniTrust C = CN	C061C3D053C9F412C5C9192DBB638305E4CA7EF8	6B661B964F2359C4CA68355243A2EEEDA9BACDA191D103A0C1119EC892018AC7	UniTrust Global SMIME RSA Root CA R1