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 as enumerated in Attachment A, SHECA has:

- disclosed its code signing ("CS") certificate lifecycle management business practices in its:
  - UniTrust Certification Practice Statement v3.7.7;
  - UniTrust Certification Practice Statement v3.7.6;
  - UniTrust Certification Practice Statement v3.7.5;
  - UniTrust Certification Practice Statement v3.7.4;
  - UniTrust Certification Practice Statement v3.7.3;
  - UniTrust Certification Practice Statement v3.7.2;
  - UniTrust Certificate Policy v1.5.5;
  - UniTrust Certificate Policy v1.5.4;
  - UniTrust Certificate Policy v1.5.3;
  - UniTrust Certificate Policy v1.5.2;
  - UniTrust Certificate Policy v1.5.1; and
  - UniTrust Certificate Policy v1.5.0,

  including its commitment to provide CS 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:
  - CS subscriber information was properly collected, authenticated (for the registration activities performed by SHECA) and verified;
  - the integrity of keys and CS certificates it manages is established and protected throughout their life cycles,

- maintained effective controls to provide reasonable assurance that its CS Timestamp Authority are operated in conformity with CA/Browser Forum Code Sign Working Group requirements v3.7.0,

- for CAs as enumerated in Attachment B are only in scope for Principle 3: Extended Validation Code Signing Service Requirements, maintained effective controls to provide reasonable assurance that:
  - EV CS subscriber information was properly collected, authenticated (for the registration activities performed by SHECA) and verified;
  - the integrity of keys and EV CS certificates it manages is established and protected throughout their life cycles,

in accordance with the WebTrust Principles and Criteria for Certification Authorities - Code Signing Baseline Requirements v3.2.

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 - Code Signing Baseline Requirements v3.2.

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 - Code Signing Baseline Requirements v3.2. 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 CS and EVCS certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of CS and EVCS certificates, and CS and EVCS Timestamp Authority certificates; (2) selectively testing transactions executed in accordance with disclosed CS and EVCS 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.

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 - Code Signing Baseline Requirements v3.2.

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 - Code Signing Baseline Requirements v3.2, 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 #9, Attachment B #5) 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 2 incidents (see Attachment C) 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.

pwc

羅兵咸永道

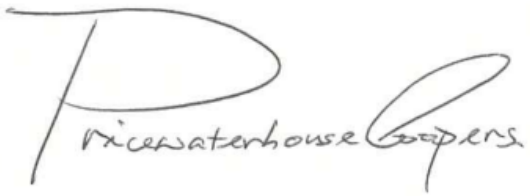
Purpose and Restriction on Use

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 - Code Signing Baseline Requirements v3.2 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 - Code Signing Baseline Requirements v3.2.

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

SHECA's use of the WebTrust for Certification Authorities - Code Signing 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

[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.*

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	9BEA11C976FE014764C1BE56A6F914B5A560317ABD9988393382E5161AA0493C	UCA Global G2 Root
2	SHECA RSA Code Signing CA G3	Signing Key	sha256RSA	2048 bits	CN = SHECA RSA Code Signing CA G3 O = UniTrust C = CN	FD7EC87AC2771C5687D2AEF807C7426A1B7C42A8	C7E976AA77E92491C269840B2F1461E65147A2BB181EE59AB63BCD86704FE456	UCA Global G2 Root
3	SHECA Code Signing CA G4	Signing Key	sha256RSA	3072 bits	CN = SHECA Code Signing CA G4 O = UniTrust C = CN	73C3B39021CBF23BDA23D351F295C58BC678EE47	8F0C3E06A16E3EA7C9B15A848076ED15E51DA0B6F1AFA274EDE2B9102191FE0F	UCA Global G2 Root
4	SHECA Global G3 Code Signing	Signing Key	sha256RSA	2048 bits	CN = SHECA Global G3 Code Signing O = UniTrust S = Shanghai C = CN	F73DF939A8D98754AC778EF5D995EEF835AB9439	EAA5AD8E9A2FA992354B2FF4254BEB08A632F7F17602604DDED58D73D616D844	UCA Global G2 Root
5	UCA Extended Validation Root	Root Key	sha256RSA	4096 bits	CN = UCA Extended Validation Root O = UniTrust C = CN	D9743AE4303D0DF712DC7E5A059F1E349AF7E114	D43AF9B35473755C9684FC06D7D8CB70EE5C28E773FB294EB41EE71722924D24	UCA Extended Validation Root
6	SHECA RSA Extended Validation Code Signing CA	Signing Key	sha256RSA	2048 bits	CN = SHECA RSA Extended Validation Code Signing CA O = UniTrust C = CN	8E40665F6AA940C2B9F1F04A22639564593707E5	D404FAFA4BA2F426B66CD219C6DA84F91C0FB7CB58429EC8077E2A764314D55D	UCA Extended Validation Root
7	SHECA EV Code Signing CA G2	Signing Key	sha256RSA	3072 bits	CN = SHECA EV Code Signing CA G2 O = UniTrust C = CN	5007CC4DF6F4BA37FC13CE1F2D22C956D89EA503	DD84169585A2E7A216AECD4083265A8EB51A64F7C6F1943671F8584C73F79A74	UCA Extended Validation Root
8	SHECA Extended Validation Code Signing CA	Signing Key	sha256RSA	2048 bits	CN = SHECA Extended Validation Code Signing CA O = UniTrust C = CN	7498996F6A15C0062520851CAF2B316B87EDA3DB	A392C645B9A5AD6A214F19DE776346BC7DD6BB15818E433886DAC54EE6661852	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
9	UniTrust Global Root CA R1	Root Key	sha384RSA	4096 bits	CN = UniTrust Global Root CA R1 O = UniTrust C = CN	3CA061B0EF DAC6E8BB2D E156A2EBBBB 63D232381	81B35EFC42C7794 7209D76B51B5E7B 122CE78348AE8C4 525DC8D4B30289 E5385	UniTrust Global Root CA R1
10	SHECA Code Signing CA 1A	Signing Key	sha384RSA	4096 bits	CN = SHECA Code Signing CA 1A O = UniTrust C = CN	21B34B4FC6D D33246E861B ACEBF182D7 EFCA2CDA	59E3EF6680BCC0 B1162DED4929D37 E698C6A5CBEE07 5C03F1173AD653C F91CED	UniTrust Global Root CA R1
11	SHECA EV Code Signing CA 1A	Signing Key	sha384RSA	4096 bits	CN = SHECA EV Code Signing CA 1A O = UniTrust C = CN	510BE3C14EA BDFEA38FF4 34E2C97339C 0BFC27A9	03E04A3C2B5200 BB27C679A372618 52BAC7D46F3F371 E4ECA80225AE28 8E4CFC	UniTrust Global Root CA R1
12	UniTrust Global Code Signing ECC Root CA R2	Root Key	sha384ECDSA	384 bits	CN = UniTrust Global Code Signing ECC Root CA R2 O = UniTrust C = CN	D6E2F5C7B44 0515C5A3A5C 490EFCB8C23 9503CDB	8854E81F9C6B47E 438BBAE17E41F8B E4E68589AFD31A4 8BEE3F203F6DD3 DA517	UniTrust Global Code Signing ECC Root CA R2
13	SHECA Code Signing ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA Code Signing ECC CA 2A O = UniTrust C = CN	3A5576122E3 85EB715671E E385BF1E3D0 AC77A1A	953707AE07AF349 70462E8C02AC3D1 0949D3684D06338 5277F31869508007 D23	UniTrust Global Code Signing ECC Root CA R2
14	SHECA EV Code Signing ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA EV Code Signing ECC CA 2A O = UniTrust C = CN	BFAE7906E97 76B61D01E45 79986F2698B 66DF25E	545BD126658352B 306EE74185173F17 74A79467A26E9BB 6AE0ED44D86615 DE5A	UniTrust Global Code Signing ECC Root CA R2
15	UniTrust Global Code Signing RSA Root CA R1	Root Key	sha384RSA	4096 bits	CN = UniTrust Global Code Signing RSA Root CA R1 O = UniTrust C = CN	60C14C87BDA AB27B678E4E A7921C519B4 81BA860	6357353A4BBCA3D 5A158C95BE9DC90 F0B3E2F6A6310FD 5371FCB4C41E5E1B B4C	UniTrust Global Code Signing RSA Root CA R1
16	UniTrust Global Time Stamping ECC Root CA R2	Root Key	sha384ECDSA	384 bits	CN = UniTrust Global Time Stamping ECC Root CA R2 O = UniTrust C = CN	C20E70D5E4 015590A717B6 2DDDB5389D 7627A1B7	90711D905CFF3C7 73A7320B5188A96 0C8A7D9E5966FA7 3284D64A4BF3E2F DA48	UniTrust Global Time Stamping ECC Root CA R2
17	SHECA Time Stamping ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA Time Stamping ECC CA 2A O = UniTrust C = CN	41315BE8FD8 C3C65630168 307A0B30EC 097F1069	0E3FC096DDCC32 05047F9042D5788 2A1144107243C47C DE6FFFDE403A5B 7CA04	UniTrust Global Time Stamping ECC Root CA R2

#	Key Name	Key Type	Signature Algorithm	Key Size	Subject DN	Subject Key Identifier	Certificates Thumbprint (SHA256)	Certificate Signed by
18	UniTrust Global Time Stamping RSA Root CA R1	Root Key	sha384RSA	4096 bits	CN = UniTrust Global Time Stamping RSA Root CA R1 O = UniTrust C = CN	DA891E9DC30F38DAB0896CCDC5FDD7504F155B30	1759727D9E6679B069DD3AFA910E2779C42007AAB206A169C66E6E2A3D1774B0	UniTrust Global Time Stamping RSA Root CA R1

Attachment B

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 Extended Validation Root	Root Key	sha256RSA	4096 bits	CN = UCA Extended Validation Root O = UniTrust C = CN	D9743AE4303D0DF712DC7E5A059F1E349AF7E114	D43AF9B35473755C9684FC06D7D8CB70EE5C28E773FB294EB41EE71722924D24	UCA Extended Validation Root
2	SHECA RSA Extended Validation Code Signing CA	Signing Key	sha256RSA	2048 bits	CN = SHECA RSA Extended Validation Code Signing CA O = UniTrust C = CN	8E40665F6AA940C2B9F1F04A22639564593707E5	D404FAFA4BA2F426B66CD219C6DA84F91C0FB7CB58429EC8077E2A764314D55D	UCA Extended Validation Root
3	SHECA EV Code Signing CA G2	Signing Key	sha256RSA	3072 bits	CN = SHECA EV Code Signing CA G2 O = UniTrust C = CN	5007CC4DF6F4BA37FC13CE1F2D22C956D89EA503	DD84169585A2E7A216AECD4083265A8EB51A64F7C6F1943671F8584C73F79A74	UCA Extended Validation Root
4	SHECA Extended Validation Code Signing CA	Signing Key	sha256RSA	2048 bits	CN = SHECA Extended Validation Code Signing CA O = UniTrust C = CN	7498996F6A15C0062520851CAF2B316B87EDA3DB	A392C645B9A5AD6A214F19DE776346BC7DD6BB15818E433886DAC54EE6661852	UCA Extended Validation Root
5	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
6	SHECA EV Code Signing CA 1A	Signing Key	sha384RSA	4096 bits	CN = SHECA EV Code Signing CA 1A O = UniTrust C = CN	510BE3C14EABDFEA38FF434E2C97339C0BFC27A9	03E04A3C2B5200BB27C679A37261852BAC7D46F3F371E4ECA80225AE288E4CFC	UniTrust Global Root CA R1

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
7	UniTrust Global Code Signing ECC Root CA R2	Root Key	sha384ECDSA	384 bits	CN = UniTrust Global Code Signing ECC Root CA R2 O = UniTrust C = CN	D6E2F5C7B440515C5A3A5C490EFCB8C239503CDB	8854E81F9C6B47E438BBAE17E41F8BE4E68589AFD31A48BEE3F203F6DD3DA517	UniTrust Global Code Signing ECC Root CA R2
8	SHECA EV Code Signing ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA EV Code Signing ECC CA 2A O = UniTrust C = CN	BFAE7906E9776B61D01E4579986F2698B66DF25E	545BD126658352B306EE74185173F1774A79467A26E9BB6AE0ED44D86615DE5A	UniTrust Global Code Signing ECC Root CA R2
9	UniTrust Global Code Signing RSA Root CA R1	Root Key	sha384RSA	4096 bits	CN = UniTrust Global Code Signing RSA Root CA R1 O = UniTrust C = CN	60C14C87BDAAB27B678E4EA7921C519B481BA860	6357353A4BBCA3D5A158C95BE9DC90F0B3E2F6A6310FD5371FCB4C41E5E1BB4C	UniTrust Global Code Signing RSA Root CA R1

pwc

羅兵咸永道

Attachment C - 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

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 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）运营的代码签名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：

- 披露代码签名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证书认证业务规则 v3.7.5;
  - UniTrust证书认证业务规则v3.7.4;
  - UniTrust证书认证业务规则 v3.7.3;
  - UniTrust证书认证业务规则 v3.7.2;
  - UniTrust证书策略 v1.5.5;
  - UniTrust证书策略v1.5.4;
  - UniTrust证书策略 v1.5.3;
  - UniTrust证书策略 v1.5.2;
  - UniTrust证书策略 v1.5.1; 以及
  - UniTrust证书策略 v1.5.0,

  包括承诺遵循CAB论坛（CA/Browser Forum）的相关指引提供代码签名服务，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；
  - 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，对代码签名时间戳服务的操作符合 CA/Browser Forum Code Sign Working Group requirements v3.7.0 提供合理保证，

- 并且，对于附录B中所包括的仅符合原则3的根证书和中级证书：通过有效控制机制，对增强代码签名的操作符合增强代码签名要求提供以下合理保证：
  - 恰当地鉴定（SHECA 所执行的注册操作）代码签名增强验证证书申请者的信息；以及
  - 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，

以符合 WebTrust电子认证代码签名基准规范审计标准 v3.2。

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 - 代码签名基准规范审计标准v3.2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 - 代码签名基准规范审计标准 v3.2 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 代码签名证书生命周期管理，包括代码签名证书发放、更新和吊销，代码签名签名机构证书管理，以及代码签名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。

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 - 代码签名基准规范审计标准 v3.2。

pwc 羅兵咸永道

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 - 代码签名基准规范审计标准 v3.2 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#9，附录 B#5）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 2 起事件（见附录 C）。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 - 代码签名基准规范审计标准 v3.2，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 - 代码签名基准规范审计标准 v3.2 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 RSA Code Signing CA G3	Signing Key	sha256RSA	2048 bits	CN = SHECA RSA Code Signing CA G3 O = UniTrust C = CN	FD7EC87AC2771C5687D2AEF807C7426A1B7C42A8	C7E976AA77E92491C269840B2F1461E65147A2BB181EE59AB63BCD86704FE456	UCA Global G2 Root
3	SHECA Code Signing CA G4	Signing Key	sha256RSA	3072 bits	CN = SHECA Code Signing CA G4 O = UniTrust C = CN	73C3B39021CBF23BDA23D351F295C58BC678EE47	8F0C3E06A16E3EA7C9B15A848076ED15E51DA0B6F1AFA274EDE2B9102191FE0F	UCA Global G2 Root
4	SHECA Global G3 Code Signing	Signing Key	sha256RSA	2048 bits	CN = SHECA Global G3 Code Signing O = UniTrust S = Shanghai C = CN	F73DF939A8D98754AC778EF5D995EEF835AB9439	EAA5AD8E9A2FA992354B2FF4254BEB08A632F7F17602604DDED58D73D616D844	UCA Global G2 Root
5	UCA Extended Validation Root	Root Key	sha256RSA	4096 bits	CN = UCA Extended Validation Root O = UniTrust C = CN	D9743AE4303D0DF712DC7E5A059F1E349AF7E114	D43AF9B35473755C9684FC06D7D8CB70EE5C28E773FB294EB41EE71722924D24	UCA Extended Validation Root
6	SHECA RSA Extended Validation Code Signing CA	Signing Key	sha256RSA	2048 bits	CN = SHECA RSA Extended Validation Code Signing CA O = UniTrust C = CN	8E40665F6AA940C2B9F1F04A22639564593707E5	D404FAFA4BA2F426B66CD219C6DA84F91C0FB7CB58429EC8077E2A764314D55D	UCA Extended Validation Root
7	SHECA EV Code Signing CA G2	Signing Key	sha256RSA	3072 bits	CN = SHECA EV Code Signing CA G2 O = UniTrust C = CN	5007CC4DF6F4BA37FC13CE1F2D22C956D89EA503	DD84169585A2E7A216AECD4083265A8EB51A64F7C6F1943671F8584C73F79A74	UCA Extended Validation Root
8	SHECA Extended Validation Code Signing CA	Signing Key	sha256RSA	2048 bits	CN = SHECA Extended Validation Code Signing CA O = UniTrust C = CN	7498996F6A15C0062520851CAF2B316B87EDA3DB	A392C645B9A5AD6A214F19DE776346BC7DD6BB15818E433886DAC54EE6661852	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
9	UniTrust Global Root CA R1	Root Key	sha384RSA	4096 bits	CN = UniTrust Global Root CA R1 O = UniTrust C = CN	3CA061B0EF DAC6E8BB2D E156A2EBBBB 63D232381	81B35EFC42C7794 7209D76B51B5E7B 122CE78348AE8C4 525DC8D4B30289 E5385	UniTrust Global Root CA R1
10	SHECA Code Signing CA 1A	Signing Key	sha384RSA	4096 bits	CN = SHECA Code Signing CA 1A O = UniTrust C = CN	21B34B4FC6D D33246E861B ACEBF182D7 EFCA2CDA	59E3EF6680BCC0 B1162DED4929D37 E698C6A5CBEE07 5C03F1173AD653C F91CED	UniTrust Global Root CA R1
11	SHECA EV Code Signing CA 1A	Signing Key	sha384RSA	4096 bits	CN = SHECA EV Code Signing CA 1A O = UniTrust C = CN	510BE3C14EA BDFEA38FF4 34E2C97339C 0BFC27A9	03E04A3C2B5200 BB27C679A372618 52BAC7D46F3F371 E4ECA80225AE28 8E4CFC	UniTrust Global Root CA R1
12	UniTrust Global Code Signing ECC Root CA R2	Root Key	sha384ECDSA	384 bits	CN = UniTrust Global Code Signing ECC Root CA R2 O = UniTrust C = CN	D6E2F5C7B44 0515C5A3A5C 490EFCB8C23 9503CDB	8854E81F9C6B47E 438BBAE17E41F8B E4E68589AFD31A4 8BEE3F203F6DD3 DA517	UniTrust Global Code Signing ECC Root CA R2
13	SHECA Code Signing ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA Code Signing ECC CA 2A O = UniTrust C = CN	3A5576122E3 85EB715671E E385BF1E3D0 AC77A1A	953707AE07AF349 70462E8C02AC3D1 0949D3684D06338 5277F31869508007 D23	UniTrust Global Code Signing ECC Root CA R2
14	SHECA EV Code Signing ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA EV Code Signing ECC CA 2A O = UniTrust C = CN	BFAE7906E97 76B61D01E45 79986F2698B 66DF25E	545BD126658352B 306EE74185173F17 74A79467A26E9BB 6AE0ED44D86615 DE5A	UniTrust Global Code Signing ECC Root CA R2
15	UniTrust Global Code Signing RSA Root CA R1	Root Key	sha384RSA	4096 bits	CN = UniTrust Global Code Signing RSA Root CA R1 O = UniTrust C = CN	60C14C87BDA AB27B678E4E A7921C519B4 81BA860	6357353A4BBCA3D 5A158C95BE9DC90 F0B3E2F6A6310FD 5371FCB4C41E5E1B B4C	UniTrust Global Code Signing RSA Root CA R1
16	UniTrust Global Time Stamping ECC Root CA R2	Root Key	sha384ECDSA	384 bits	CN = UniTrust Global Time Stamping ECC Root CA R2 O = UniTrust C = CN	C20E70D5E4 015590A717B6 2DDDB5389D 7627A1B7	90711D905CFF3C7 73A7320B5188A96 0C8A7D9E5966FA7 3284D64A4BF3E2F DA48	UniTrust Global Time Stamping ECC Root CA R2
17	SHECA Time Stamping ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA Time Stamping ECC CA 2A O = UniTrust C = CN	41315BE8FD8 C3C65630168 307A0B30EC 097F1069	0E3FC096DDCC32 05047F9042D5788 2A1144107243C47C DE6FFFDE403A5B 7CA04	UniTrust Global Time Stamping ECC Root CA R2
18	UniTrust Global Time Stamping	Root Key	sha384RSA	4096 bits	CN = UniTrust Global Time Stamping RSA Root CA R1	DA891E9DC3 0F38DAB089 6CCDC5FDD7 504F155B30	1759727D9E6679B0 69DD3AFA910E277 9C42007AAB206A1	UniTrust Global Time Stamping 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
	RSA Root CA R1				O = UniTrust C = CN		69C66E6E2A3D1774B0	

附录 B

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 Extended Validation Root	Root Key	sha256RSA	4096 bits	CN = UCA Extended Validation Root O = UniTrust C = CN	D9743AE4303D0DF712DC7E5A059F1E349AF7E114	D43AF9B35473755C9684FC06D7D8CB70EE5C28E773FB294EB41EE71722924D24	UCA Extended Validation Root
2	SHECA RSA Extended Validation Code Signing CA	Signing Key	sha256RSA	2048 bits	CN = SHECA RSA Extended Validation Code Signing CA O = UniTrust C = CN	8E40665F6AA940C2B9F1F04A22639564593707E5	D404FAFA4BA2F426B66CD219C6DA84F91C0FB7CB58429EC8077E2A764314D55D	UCA Extended Validation Root
3	SHECA EV Code Signing CA G2	Signing Key	sha256RSA	3072 bits	CN = SHECA EV Code Signing CA G2 O = UniTrust C = CN	5007CC4DF6F4BA37FC13CE1F2D22C956D89EA503	DD84169585A2E7A216AECD4083265A8EB51A64F7C6F1943671F8584C73F79A74	UCA Extended Validation Root
4	SHECA Extended Validation Code Signing CA	Signing Key	sha256RSA	2048 bits	CN = SHECA Extended Validation Code Signing CA O = UniTrust C = CN	7498996F6A15C0062520851CAF2B316B87EDA3DB	A392C645B9A5AD6A214F19DE776346BC7DD6BB15818E433886DAC54EE6661852	UCA Extended Validation Root
5	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
6	SHECA EV Code Signing CA 1A	Signing Key	sha384RSA	4096 bits	CN = SHECA EV Code Signing CA 1A O = UniTrust C = CN	510BE3C14EABDFEA38FF434E2C97339C0BFC27A9	03E04A3C2B5200BB27C679A37261852BAC7D46F3F371E4ECA80225AE288E4CFC	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
7	UniTrust Global Code Signing ECC Root CA R2	Root Key	sha384ECDSA	384 bits	CN = UniTrust Global Code Signing ECC Root CA R2 O = UniTrust C = CN	D6E2F5C7B440515C5A3A5C490EFCB8C239503CDB	8854E81F9C6B47E438BBAE17E41F8BE4E68589AFD31A48BEE3F203F6DD3DA517	UniTrust Global Code Signing ECC Root CA R2
8	SHECA EV Code Signing ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA EV Code Signing ECC CA 2A O = UniTrust C = CN	BFAE7906E9776B61D01E4579986F2698B66DF25E	545BD126658352B306EE74185173F1774A79467A26E9BB6AE0ED44D86615DE5A	UniTrust Global Code Signing ECC Root CA R2
9	UniTrust Global Code Signing RSA Root CA R1	Root Key	sha384RSA	4096 bits	CN = UniTrust Global Code Signing RSA Root CA R1 O = UniTrust C = CN	60C14C87BDAAB27B678E4EA7921C519B481BA860	6357353A4BBCA3D5A158C95BE9DC90F0B3E2F6A6310FD5371FCB4C41E5E1BB4C	UniTrust Global Code Signing RSA Root CA R1

附录 C – 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

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 - Code Signing 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 Appendix A), and provides Code Signing ("CS") CA services.

The management of SHECA is responsible for establishing and maintaining effective controls over its code signing services, including its code signing business practices disclosure on its website, code signing key lifecycle management controls, code signing 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 CS CA services. Based on that assessment, in SHECA management's opinion, in providing its CS 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 code signing certificate lifecycle management business practices in its:
  - UniTrust Certification Practice Statement v3.7.7;
  - UniTrust Certification Practice Statement v3.7.6;
  - UniTrust Certification Practice Statement v3.7.5;
  - UniTrust Certification Practice Statement v3.7.4;
  - UniTrust Certification Practice Statement v3.7.3;
  - UniTrust Certification Practice Statement v3.7.2;
  - UniTrust Certificate Policy v1.5.5;
  - UniTrust Certificate Policy v1.5.4;
  - UniTrust Certificate Policy v1.5.3;
  - UniTrust Certificate Policy v1.5.2;

- UniTrust Certificate Policy v1.5.1; and
- UniTrust Certificate Policy v1.5.0,

including its commitment to provide CS certificates in conformity with the applicable Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates, and provided such services in accordance with its disclosed practices,

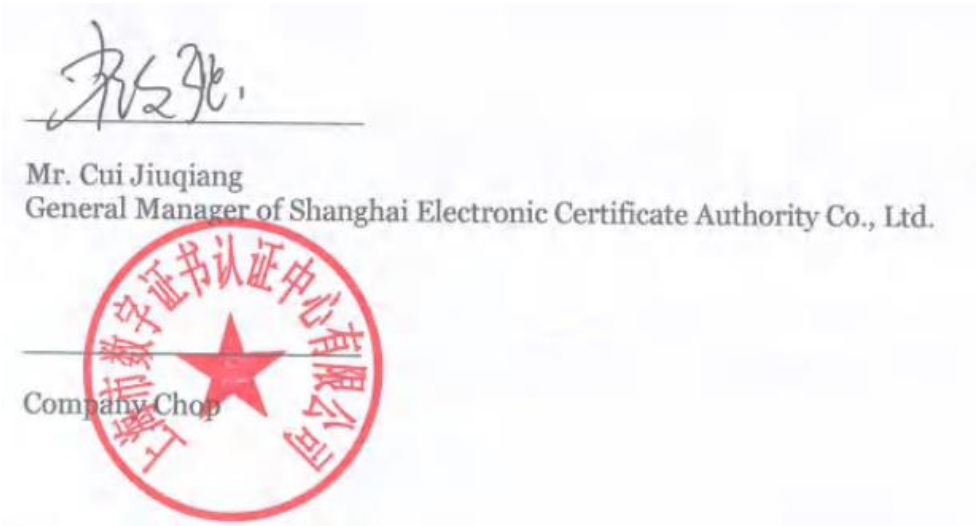
- maintained effective controls to provide reasonable assurance that:
  - CS subscriber information was properly collected, authenticated (for the registration activities performed by SHECA) and verified;
  - the integrity of keys and CS certificates it manages is established and protected throughout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

- maintained effective controls to provide reasonable assurance that its CS Timestamp Authority are operated in conformity with CA/Browser Forum Code Sign Working Group requirements v3.7.0.

- for CAs as enumerated in Appendix B are only in scope for Principle 3: Extended Validation Code Signing Service Requirements, maintained effective controls to provide reasonable assurance that:
  - EV CS subscriber information was properly collected, authenticated (for the registration activities performed by SHECA) and verified;
  - the integrity of keys and EV CS certificates it manages is established and protected throughout their life cycles,

in accordance with the WebTrust Principles and Criteria for Certification Authorities - Code Signing Baseline Requirements v3.2.

The UniTrust Global Root CA R1 (Appendix A #9, Appendix B #5) 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.



Appendix A

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 RSA Code Signing CA G3	Signing Key	sha256RSA	2048 bits	CN = SHECA RSA Code Signing CA G3 O = UniTrust C = CN	FD7EC87AC2771C5687D2AEF807C7426A1B7C42A8	C7E976AA77E92491C269840B2F1461E65147A2BB181EE59AB63BCD86704FE456	UCA Global G2 Root
3	SHECA Code Signing CA G4	Signing Key	sha256RSA	3072 bits	CN = SHECA Code Signing CA G4 O = UniTrust C = CN	73C3B39021CBF23BDA23D351F295C58BC678EE47	8F0C3E06A16E3EA7C9B15A848076ED15E51DA0B6F1AFA274EDE2B9102191FE0F	UCA Global G2 Root
4	SHECA Global G3 Code Signing	Signing Key	sha256RSA	2048 bits	CN = SHECA Global G3 Code Signing O = UniTrust S = Shanghai C = CN	F73DF939A8D98754AC778EF5D995EEF835AB9439	EAA5AD8E9A2FA992354B2FF4254BEB08A632F7F17602604DDED58D73D616D844	UCA Global G2 Root
5	UCA Extended Validation Root	Root Key	sha256RSA	4096 bits	CN = UCA Extended Validation Root O = UniTrust C = CN	D9743AE4303D0DF712DC7E5A059F1E349AF7E114	D43AF9B35473755C9684FC06D7D8CB70EE5C28E773FB294EB41EE71722924D24	UCA Extended Validation Root
6	SHECA RSA Extended Validation Code Signing CA	Signing Key	sha256RSA	2048 bits	CN = SHECA RSA Extended Validation Code Signing CA O = UniTrust C = CN	8E40665F6AA940C2B9F1F04A22639564593707E5	D404FAFA4BA2F426B66CD219C6DA84F91C0FB7CB58429EC8077E2A764314D55D	UCA Extended Validation Root
7	SHECA EV Code Signing CA G2	Signing Key	sha256RSA	3072 bits	CN = SHECA EV Code Signing CA G2 O = UniTrust C = CN	5007CC4DF6F4BA37FC13CE1F2D22C956D89EA503	DD84169585A2E7A216AECD4083265A8EB51A64F7C6F1943671F8584C73F79A74	UCA Extended Validation Root
8	SHECA Extended Validation Code Signing CA	Signing Key	sha256RSA	2048 bits	CN = SHECA Extended Validation Code Signing CA O = UniTrust C = CN	7498996F6A15C0062520851CAF2B316B87EDA3DB	A392C645B9A5AD6A214F19DE776346BC7DD6BB15818E433886DAC54EE6661852	UCA Extended Validation Root
9	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
10	SHECA Code Signing CA 1A	Signing Key	sha384RSA	4096 bits	CN = SHECA Code Signing CA 1A O = UniTrust C = CN	21B34B4FC6DD33246E861BACEBF182D7EFCA2CDA	59E3EF6680BCC0B1162DED4929D37E698C6A5CBEE075C03F1173AD653CF91CED	UniTrust Global Root CA R1
11	SHECA EV Code Signing CA 1A	Signing Key	sha384RSA	4096 bits	CN = SHECA EV Code Signing CA 1A O = UniTrust C = CN	510BE3C14EABDFEA38FF434E2C97339C0BFC27A9	03E04A3C2B5200BB27C679A37261852BAC7D46F3F371E4ECA80225AE288E4CFC	UniTrust Global Root CA R1
12	UniTrust Global Code Signing ECC Root CA R2	Root Key	sha384ECDSA	384 bits	CN = UniTrust Global Code Signing ECC Root CA R2 O = UniTrust C = CN	D6E2F5C7B440515C5A3A5C490EFCB8C239503CDB	8854E81F9C6B47E438BBAE17E41F8BE4E68589AFD31A48BEE3F203F6DD3DA517	UniTrust Global Code Signing ECC Root CA R2
13	SHECA Code Signing ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA Code Signing ECC CA 2A O = UniTrust C = CN	3A5576122E385EB715671EE385BF1E3D0AC77A1A	953707AE07AF34970462E8C02AC3D10949D3684D063385277F31869508007D23	UniTrust Global Code Signing ECC Root CA R2
14	SHECA EV Code Signing ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA EV Code Signing ECC CA 2A O = UniTrust C = CN	BFAE7906E9776B61D01E4579986F2698B66DF25E	545BD126658352B306EE74185173F1774A79467A26E9BB6AE0ED44D86615DE5A	UniTrust Global Code Signing ECC Root CA R2
15	UniTrust Global Code Signing RSA Root CA R1	Root Key	sha384RSA	4096 bits	CN = UniTrust Global Code Signing RSA Root CA R1 O = UniTrust C = CN	60C14C87BDAAB27B678E4EA7921C519B481BA860	6357353A4BBCA3D5A158C95BE9DC90F0B3E2F6A6310FD5371FCB4C41E5E1BB4C	UniTrust Global Code Signing RSA Root CA R1
16	UniTrust Global Time Stamping ECC Root CA R2	Root Key	sha384ECDSA	384 bits	CN = UniTrust Global Time Stamping ECC Root CA R2 O = UniTrust C = CN	C20E70D5E4015590A717B62DDDB5389D7627A1B7	90711D905CFF3C773A7320B5188A960C8A7D9E5966FA73284D64A4BF3E2FDA48	UniTrust Global Time Stamping ECC Root CA R2
17	SHECA Time Stamping ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA Time Stamping ECC CA 2A O = UniTrust C = CN	41315BE8FD8C3C65630168307A0B30EC097F1069	0E3FC096DDCC3205047F9042D57882A1144107243C47CDE6FFFDE403A5B7CA04	UniTrust Global Time Stamping ECC Root CA R2
18	UniTrust Global Time Stamping RSA Root CA R1	Root Key	sha384RSA	4096 bits	CN = UniTrust Global Time Stamping RSA Root CA R1 O = UniTrust C = CN	DA891E9DC30F38DAB0896CCDC5FDD7504F155B30	1759727D9E6679B069DD3AFA910E2779C42007AAB206A169C66E6E2A3D1774B0	UniTrust Global Time Stamping RSA Root CA R1

Appendix B

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 Extended Validation Root	Root Key	sha256RSA	4096 bits	CN = UCA Extended Validation Root O = UniTrust C = CN	D9743AE4303D0DF712DC7E5A059F1E349AF7E114	D43AF9B35473755C9684FC06D7D8CB70EE5C28E773FB294EB41EE71729924D24	UCA Extended Validation Root
2	SHECA RSA Extended Validation Code Signing CA	Signing Key	sha256RSA	2048 bits	CN = SHECA RSA Extended Validation Code Signing CA O = UniTrust C = CN	8E40665F6AA940C2B9F1F04A22639564593707E5	D404FAFA4BA2F426B66CD219C6DA84F91C0FB7CB58429EC8077E2A764314D55D	UCA Extended Validation Root
3	SHECA EV Code Signing CA G2	Signing Key	sha256RSA	3072 bits	CN = SHECA EV Code Signing CA G2 O = UniTrust C = CN	5007CC4DF6F4BA37FC13CE1F2D22C956D89EA503	DD84169585A2E7A216AECD4083265A8EB51A64F7C6F1943671F8584C73F79A74	UCA Extended Validation Root
4	SHECA Extended Validation Code Signing CA	Signing Key	sha256RSA	2048 bits	CN = SHECA Extended Validation Code Signing CA O = UniTrust C = CN	7498996F6A15C0062520851CAF2B316B87EDA3DB	A392C645B9A5AD6A214F19DE776346BC7DD6BB15818E433886DAC54EE6661852	UCA Extended Validation Root
5	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
6	SHECA EV Code Signing CA 1A	Signing Key	sha384RSA	4096 bits	CN = SHECA EV Code Signing CA 1A O = UniTrust C = CN	510BE3C14EABDFEA38FF434E2C97339C0BFC27A9	03E04A3C2B5200BB27C679A37261852BAC7D46F3F371E4ECA80225AE288E4CFC	UniTrust Global Root CA R1
7	UniTrust Global Code Signing ECC Root CA R2	Root Key	sha384ECDSA	384 bits	CN = UniTrust Global Code Signing ECC Root CA R2 O = UniTrust C = CN	D6E2F5C7B440515C5A3A5C490EFCB8C239503CDB	8854E81F9C6B47E438BBAE17E41F8BE4E68589AFD31A48BEE3F203F6DD3DA517	UniTrust Global Code Signing ECC Root CA R2
8	SHECA EV Code Signing ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA EV Code Signing ECC CA 2A O = UniTrust C = CN	BFAE7906E9776B61D01E4579986F2698B66DF25E	545BD126658352B306EE74185173F1774A79467A26E9BB6AE0ED44D86615DE5A	UniTrust Global Code Signing ECC Root CA R2
9	UniTrust Global Code Signing RSA Root CA R1	Root Key	sha384RSA	4096 bits	CN = UniTrust Global Code Signing RSA Root CA R1 O = UniTrust C = CN	60C14C87BDAAB27B678E4EA7921C519B481BA860	6357353A4BBCA3D5A158C95BE9DC90F0B3E2F6A6310FD5371FCB4C41E5E1BB4C	UniTrust Global Code Signing 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 日期间代码签名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，并提供代码签名电子认证服务，附录 A 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服务建立并维护有效的控制，包括：披露代码签名业务规则，代码签名密钥生命周期管理，代码签名证书生命周期管理和代码签名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）提供的代码签名电子认证服务期间，SHECA：

- 披露代码签名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证书认证业务规则 v3.7.5;
  - UniTrust证书认证业务规则 v3.7.4;
  - UniTrust证书认证业务规则 v3.7.3;
  - UniTrust证书认证业务规则 v3.7.2;
  - UniTrust证书策略 v1.5.5;
  - UniTrust证书策略 v1.5.4;
  - UniTrust证书策略 v1.5.3;
  - UniTrust证书策略 v1.5.2;

- UniTrust证书策略 v1.5.1; 以及
- UniTrust证书策略 v1.5.0,

包括承诺遵循CAB论坛（CA/Browser Forum）的相关指引提供代码签名服务，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，对代码签名证书及代码签名时间戳服务的操作符合 CA/Browser Forum Code Sign Working Group requirements v3.7.0.

- 并且，对于附录B中所包括的仅符合原则3的根证书和中级证书：通过有效控制机制，对增强代码签名的操作符合增强代码签名要求提供以下合理保证：
  - 恰当地鉴定（SHECA所执行的注册操作）代码签名增强验证证书申请者的信息；以及
  - 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

以符合 WebTrust电子认证代码签名基准规范审计标准v3.2.

UniTrust Global Root CA R1（附录 A#9，附录 B#5）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 A

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 RSA Code Signing CA G3	Signing Key	sha256RSA	2048 bits	CN = SHECA RSA Code Signing CA G3 O = UniTrust C = CN	FD7EC87AC2771C5687D2AEF807C7426A1B7C42A8	C7E976AA77E92491C269840B2F1461E65147A2BB181EE59AB63BCD86704FE456	UCA Global G2 Root
3	SHECA Code Signing CA G4	Signing Key	sha256RSA	3072 bits	CN = SHECA Code Signing CA G4 O = UniTrust C = CN	73C3B39021CBF23BDA23D351F295C58BC678EE47	8F0C3E06A16E3EA7C9B15A848076ED15E51DA0B6F1AFA274EDE2B9102191FE0F	UCA Global G2 Root
4	SHECA Global G3 Code Signing	Signing Key	sha256RSA	2048 bits	CN = SHECA Global G3 Code Signing O = UniTrust S = Shanghai C = CN	F73DF939A8D98754AC778EF5D995EEF835AB9439	EAA5AD8E9A2FA992354B2FF4254BEB08A632F7F17602604DDED58D73D616D844	UCA Global G2 Root
5	UCA Extended Validation Root	Root Key	sha256RSA	4096 bits	CN = UCA Extended Validation Root O = UniTrust C = CN	D9743AE4303D0DF712DC7E5A059F1E349AF7E114	D43AF9B35473755C9684FC06D7D8CB70EE5C28E773FB294EB41EE71722924D24	UCA Extended Validation Root
6	SHECA RSA Extended Validation Code Signing CA	Signing Key	sha256RSA	2048 bits	CN = SHECA RSA Extended Validation Code Signing CA O = UniTrust C = CN	8E40665F6AA940C2B9F1F04A22639564593707E5	D404FAFA4BA2F426B66CD219C6DA84F91C0FB7CB58429EC8077E2A764314D55D	UCA Extended Validation Root
7	SHECA EV Code Signing CA G2	Signing Key	sha256RSA	3072 bits	CN = SHECA EV Code Signing CA G2 O = UniTrust C = CN	5007CC4DF6F4BA37FC13CE1F2D22C956D89EA503	DD84169585A2E7A216AECD4083265A8EB51A64F7C6F1943671F8584C73F79A74	UCA Extended Validation Root
8	SHECA Extended Validation Code Signing CA	Signing Key	sha256RSA	2048 bits	CN = SHECA Extended Validation Code Signing CA O = UniTrust C = CN	7498996F6A15C0062520851CAF2B316B87EDA3DB	A392C645B9A5AD6A214F19DE776346BC7DD6BB15818E433886DAC54EE6661852	UCA Extended Validation Root
9	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
10	SHECA Code Signing CA 1A	Signing Key	sha384RSA	4096 bits	CN = SHECA Code Signing CA 1A O = UniTrust C = CN	21B34B4FC6DD33246E861BACEBF182D7EFCA2CDA	59E3EF6680BCC0B1162DED4929D37E698C6A5CBEE075C03F1173AD653CF91CED	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
11	SHECA EV Code Signing CA 1A	Signing Key	sha384RSA	4096 bits	CN = SHECA EV Code Signing CA 1A O = UniTrust C = CN	510BE3C14EABDFEA38FF434E2C97339C0BFC27A9	03E04A3C2B5200BB27C679A37261852BAC7D46F3F371E4ECA80225AE288E4CFC	UniTrust Global Root CA R1
12	UniTrust Global Code Signing ECC Root CA R2	Root Key	sha384ECDSA	384 bits	CN = UniTrust Global Code Signing ECC Root CA R2 O = UniTrust C = CN	D6E2F5C7B440515C5A3A5C490EFCB8C239503CDB	8854E81F9C6B47E438BBAE17E41F8BE4E68589AFD31A48BEE3F203F6DD3DA517	UniTrust Global Code Signing ECC Root CA R2
13	SHECA Code Signing ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA Code Signing ECC CA 2A O = UniTrust C = CN	3A5576122E385EB715671EE385BF1E3D0AC77A1A	953707AE07AF34970462E8C02AC3D10949D3684D063385277F31869508007D23	UniTrust Global Code Signing ECC Root CA R2
14	SHECA EV Code Signing ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA EV Code Signing ECC CA 2A O = UniTrust C = CN	BFAE7906E9776B61D01E4579986F2698B66DF25E	545BD126658352B306EE74185173F1774A79467A26E9BB6AE0ED44D86615DE5A	UniTrust Global Code Signing ECC Root CA R2
15	UniTrust Global Code Signing RSA Root CA R1	Root Key	sha384RSA	4096 bits	CN = UniTrust Global Code Signing RSA Root CA R1 O = UniTrust C = CN	60C14C87BDAAB27B678E4EA7921C519B481BA860	6357353A4BBCA3D5A158C95BE9DC90F0B3E2F6A6310FD5371FCB4C41E5E1BB4C	UniTrust Global Code Signing RSA Root CA R1
16	UniTrust Global Time Stamping ECC Root CA R2	Root Key	sha384ECDSA	384 bits	CN = UniTrust Global Time Stamping ECC Root CA R2 O = UniTrust C = CN	C20E70D5E4015590A717B62DDDB5389D7627A1B7	90711D905CFF3C773A7320B5188A960C8A7D9E5966FA73284D64A4BF3E2FDA48	UniTrust Global Time Stamping ECC Root CA R2
17	SHECA Time Stamping ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA Time Stamping ECC CA 2A O = UniTrust C = CN	41315BE8FD8C3C6563016830 7A0B30EC097F1069	0E3FC096DDCC3205047F9042D57882A1144107243C47CDE6FFFDE403A5B7CA04	UniTrust Global Time Stamping ECC Root CA R2
18	UniTrust Global Time Stamping RSA Root CA R1	Root Key	sha384RSA	4096 bits	CN = UniTrust Global Time Stamping RSA Root CA R1 O = UniTrust C = CN	DA891E9DC30F38DAB0896CCDC5FDD7504F155B30	1759727D9E6679B069DD3AFA910E2779C42007AAB206A169C66E6E2A3D1774B0	UniTrust Global Time Stamping RSA Root CA R1

附录 B

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 Extended Validation Root	Root Key	sha256RSA	4096 bits	CN = UCA Extended Validation Root O = UniTrust C = CN	D9743AE4303D0DF712DC7E5A059F1E349AF7E114	D43AF9B35473755C9684FC06D7D8CB70EE5C28E773FB294EB41EE71729924D24	UCA Extended Validation Root
2	SHECA RSA Extended Validation Code Signing CA	Signing Key	sha256RSA	2048 bits	CN = SHECA RSA Extended Validation Code Signing CA O = UniTrust C = CN	8E40665F6AA940C2B9F1F04A22639564593707E5	D404FAFA4BA2F426B66CD219C6DA84F91C0FB7CB58429EC8077E2A764314D55D	UCA Extended Validation Root
3	SHECA EV Code Signing CA G2	Signing Key	sha256RSA	3072 bits	CN = SHECA EV Code Signing CA G2 O = UniTrust C = CN	5007CC4DF6F4BA37FC13CE1F2D22C956D89EA503	DD84169585A2E7A216AECD4083265A8EB51A64F7C6F1943671F8584C73F79A74	UCA Extended Validation Root
4	SHECA Extended Validation Code Signing CA	Signing Key	sha256RSA	2048 bits	CN = SHECA Extended Validation Code Signing CA O = UniTrust C = CN	7498996F6A15C0062520851CAF2B316B87EDA3DB	A392C645B9A5AD6A214F19DE776346BC7DD6BB15818E433886DAC54EE6661852	UCA Extended Validation Root
5	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
6	SHECA EV Code Signing CA 1A	Signing Key	sha384RSA	4096 bits	CN = SHECA EV Code Signing CA 1A O = UniTrust C = CN	510BE3C14EABDFEA38FF434E2C97339C0BFC27A9	03E04A3C2B5200BB27C679A37261852BAC7D46F3F371E4ECA80225AE288E4CFC	UniTrust Global Root CA R1
7	UniTrust Global Code Signing ECC Root CA R2	Root Key	sha384ECDSA	384 bits	CN = UniTrust Global Code Signing ECC Root CA R2 O = UniTrust C = CN	D6E2F5C7B440515C5A3A5C490EFCB8C239503CDB	8854E81F9C6B47E438BBAE17E41F8BE4E68589AFD31A48BEE3F203F6DD3DA517	UniTrust Global Code Signing ECC Root CA R2
8	SHECA EV Code Signing ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA EV Code Signing ECC CA 2A O = UniTrust C = CN	BFAE7906E9776B61D01E4579986F2698B66DF25E	545BD126658352B306EE74185173F1774A79467A26E9BB6AE0ED44D86615DE5A	UniTrust Global Code Signing ECC Root CA R2
9	UniTrust Global Code Signing RSA Root CA R1	Root Key	sha384RSA	4096 bits	CN = UniTrust Global Code Signing RSA Root CA R1 O = UniTrust C = CN	60C14C87BDAAB27B678E4EA7921C519B481BA860	6357353A4BBCA3D5A158C95BE9DC90F0B3E2F6A6310FD5371FCB4C41E5E1BB4C	UniTrust Global Code Signing RSA Root CA R1