Independent practitioner's assurance report

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

We have been engaged to perform a reasonable assurance engagement on the accompanying management's assertion of SHECA for its certification authority operations at Shanghai (including Facility 1 and Facility 2), China for the period from May 1, 2021 to March 31, 2022.

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 - SSL Baseline with Network Security v2.5.

Our Independence and Quality Control

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 Control 1 and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Practitioner's Responsibilities

It is our responsibility to express an opinion on the 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 - SSL Baseline with Network Security v2.5. The extent of

INDEPENDENT PRACTITIONER'S ASSURANCE REPORT (CONTINUED)

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 SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of SSL certificates, and obtaining an understanding of SHECA's network and certificate system security to meet the requirements set forth by the CA/Browser Forum; (2) selectively testing transactions executed in accordance with disclosed SSL 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 May 1, 2021 to March 31, 2022, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security v2.5.

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 - SSL Baseline with Network Security v2.5, nor the suitability of any of SHECA's services for any customer's intended purpose.

INDEPENDENT PRACTITIONER'S ASSURANCE REPORT (CONTINUED)

Other Matter

SEHCA's use of the WebTrust for Certification Authorities Seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

Purpose and Restriction on Use

The 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 - SSL Baseline with Network Security v2.5 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 - SSL Baseline with Network Security v2.5. We do not assume responsibility towards or accept liability to any other person for the contents of this report.

PricewaterhouseCoopers Zhong Tian LLP

Shanghai, China

April 22, 2022

[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.*

普华永道

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

我们接受委托，对后附 SHECA 于 2021 年 5 月 1 日至 2022 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 证书管理层认定执行了合理保证的鉴证业务。

管理层的责任

SHECA的管理层负责确保管理层认定，包括其陈述的客观性以及认定中描述的SHECA所提供的服务能够符合WebTrust电子认证 - SSL基准规范与网络安全规范审计标准v2.5的规定。

我们的独立性和质量控制

我们遵守了国际会计师职业道德准则理事会颁布的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控制准则第 1 号，据此维护全面系统的质量控制体系，包括与遵守职业道德要求、专业标准和适用的法律和法规要求的书面政策与程序。

注册会计师的责任

我们的责任是在执行鉴证工作的基础上对管理层认定发表意见。

我们根据《国际鉴证业务准则第 3000 号(修订版)——历史财务信息审计或审阅以外的鉴证业务》的规定执行了鉴证工作。该准则要求我们计划和实施工作，以形成鉴证意见。

合理保证的鉴证业务涉及实施鉴证程序，以获取有关管理层认定是否在所有重大方面符合 WebTrust 电子认证 - SSL 基准规范与网络安全规范审计标准 v2.5 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 证书生命周期管理，包括 SSL 证书发放、更新和吊销，并了解 SHECA 的网络和证书系统安全是否符合 CAB 论坛的相应要求；（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。

注册会计师独立鉴证报告（续）

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 2021 年 5 月 1 日至 2022 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 基准规范与网络安全规范审计标准 v2.5。

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 基准规范与网络安全规范审计标准 v2.5 以外的质量标准声明，或对任何客户对 SHECA 服务的合适性声明。

其他事项

在 SHECA 网站上的 WebTrust 电子认证标识是本报告内容的一种符号表示，它并不是为了也不应被认为是对本报告的更新或任何进一步的保证。

目的及使用和分发限制

管理层认定为在 SHECA 网站上获取并展示 WebTrust Seal[1]编制，并采用为该目的而设计的 WebTrust 电子认证 - SSL 基准规范与网络安全规范审计标准 v2.5，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 基准规范与网络安全规范审计标准 v2.5 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。

---

[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。*

注册会计师独立鉴证报告（续）

普华永道中天会计师事务所（特殊普通合伙）
中国上海市
2022年4月22日

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

April 22, 2022

Dear Sirs,

Assertion of Management as to the Disclosure to Business Practices and Controls over the Certification Authority - SSL Operations during the period from May 1, 2021 through March 31, 2022

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 SSL Baseline Requirements and Network Security Requirements and provides SSL CA services.

SHECA management has assessed its disclosures of its certificate practices and controls over its SSL CA services. Based on that assessment, in providing its SSL Certification Authority (CA) services at Shanghai (including Facility 1 and Facility 2), China, throughout the period May 1, 2021 to March 31, 2022, SHECA has:

- disclosed its SSL certificate lifecycle management business practices in its:
  - UniTrust Certification Practice Statement v3.7.1 (https://assets-cdn.sheca.com/documents/SHECA-CPS-v3.7.1%EF%BC%88EN%EF%BC%89.pdf);
  - UniTrust Certification Practice Statement v3.7;
  - UniTrust Certification Practice Statement v3.6.9; and
  - UniTrust Certificate Policy v1.4.9 (https://assets-cdn.sheca.com/documents/SHECA-CP-v1.4.9%20%EF%BC%88EN%20).pdf);
  - UniTrust Certificate Policy v1.4.8;
  - UniTrust Certificate Policy v1.4.7,

  including its commitment to provide SSL 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 SSL certificates it manages is established and protected throughout their lifecycles; and

- SSL 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

- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

in accordance with the WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security v2.5 (https://www.cpacanada.ca/-/media/site/operational/ms-member-services/docs/webtrust/wt100bwtbr-25-110120-finalaoda.pdf?la=en&hash=11A5FE85CBF7F0E960E681DFF6FD4592FC135B4C).

崔久强

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

Company

Appendix

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

Key Name	Key Type	Signature Algorithm	Key Size	Subject Key Identifier	Certificates Thumbprint (SHA256)	Certificate Signed by
UCA Global G2 Root	Root Key	sha256RSA	4096 bits	81C48CCCF5E430F FA50C085F8C1567 217401DFDF	9BEA11C976FE014764 C1BE56A6F914B5A560 317ABD9988393382E5 161AA0493C	UCA Global G2 Root
UCA Global G2 Root	Root Key	sha256RSA	4096 bits	81C48CCCF5E430F FA50C085F8C1567 217401DFDF	C1AFC65B1E813B0E61 46E6AA5341681272AB E9A38D59F7BD1B27B 729834A0D9C	Certum Trusted Network CA
SHECA RSA Domain Validation Server CA G3	Signing Key	sha256RSA	2048 bits	057A4D756FFD0A 83B1671675773E14 C5F53C548E	0A552A65F22FF820E7 EC3D43BBF88B02ABC 34BD247E0C3505891B 6342F16A5F2	UCA Global G2 Root
SHECA RSA Organization Validation Server CA G3	Signing Key	sha256RSA	2048 bits	316068091E32F9F6 CCC06215AA7B91A F4C119D40	26FD4C4367E463D39 C71796AE4010E53380 DC93BC132FB019D671 8A6873E81F4	UCA Global G2 Root
SHECA DV Server CA G5	Signing Key	sha256RSA	2048 bits	D8E7061B645FAB3 008887A2453AAE1 1C8304BF6D	778C516DAEC700EE5 8B3581E411E5C0DD47 8663A5163A298953415 07D6E964DD	UCA Global G2 Root
SHECA OV Server CA G5	Signing Key	sha256RSA	2048 bits	0379A38D525FD4E 988921F435854250 2F4878B7E	8AB3A0ACF289E6EF7 54BE449236843D67F4 5C191BDDD66484B85 E6E60556A9AF	UCA Global G2 Root
SHECA EV Server CA G2	Signing Key	sha256RSA	2048 bits	86B148C0420A9C6 F81FC4FDCD10F18 4BAAB5A6EA	4216527163AD2CAA82 5D3BF48F61A7661D0A BC89B58AB76B23A1E1 0999F0769F	UCA Global G2 Root
TrustAsia RSA DV TLS CA - S1	Signing Key	sha256RSA	2048 bits	9432E0D48ACD1D 93E75C5372960C5 EF1F3F67972	074ADD7F1E73EB110E C8E2B78A92C51CF5A4 51135B6F7DEFC019EE 9D74BFA4D6	UCA Global G2 Root
TrustAsia RSA OV TLS CA - S1	Signing Key	sha256RSA	2048 bits	F575D48E293E17A 8A9C49EDCE6DB0 A344D132AEB	D16BA9ACB74FEE4AA 8087EE482E86E7F6F5 F55FAC502563973075 3FE1E705E3C	UCA Global G2 Root
UCA Extended Validation Root	Root Key	sha256RSA	4096 bits	D9743AE4303D0D F712DC7E5A059F1 E349AF7E114	D43AF9B35473755C96 84FC06D7D8CB70EE5 C28E773FB294EB41EE 71722924D24	UCA Extended Validation Root
SHECA RSA Extended Validation Server CA	Signing Key	sha256RSA	2048 bits	3B4B252A77372AF CB97FEDA8BDAF2 299FC5DC5F4	4FD6FA527157EEA463 689D7A4C2B934EF22 2279725413893D98472 42C85CA9DF	UCA Extended Validation Root
SHECA EV Server CA G3	Signing Key	sha256RSA	2048 bits	54E972FB78669FE 5CBF33B8F984655 53739C0B84	7EF3F89456CE636557 B20C5DFB37F98C253 A0B660D2E9E5E7845 CAF9C038C7C1	UCA Extended Validation Root
UniTrust Global Root CA R1	Root Key	sha384RSA	4096 bits	3CA061B0EFDAC6 E8BB2DE156A2EB BBB63D232381	81B35EFC42C7794720 9D76B51B5E7B122CE7 8348AE8C4525DC8D4 B30289E5385	UniTrust Global Root CA R1

Key Name	Key Type	Signature Algorithm	Key Size	Subject Key Identifier	Certificates Thumbprint (SHA256)	Certificate Signed by
SHECA DV Server CA 1A	Signing Key	sha384RSA	4096 bits	653740E0BBF43905206A8C9CA0ACB3BBD6968CA0	D3D4A040BB41A695A96E3AAD93814CF7EF219D5819206E947B44DCC5B8E5E272	UniTrust Global Root CA R1
SHECA OV Server CA 1A	Signing Key	sha384RSA	4096 bits	8CD02E82008EE2DEFF71F61A105C74A826E858D1	9A3DB0F0FB0FF4F974A4E0C510A7C13D350485B1E6CDF5A899BB24D0F499E9BD	UniTrust Global Root CA R1
SHECA EV Server CA 1A	Signing Key	sha384RSA	4096 bits	73E36DF62D862F57DF69A53687231C85E0170216	2F1CA1A5C0D7AE58C7ADFC69D4C57EE815F39C0F3D1F982E3AC76D25AB723995	UniTrust Global Root CA R1
UniTrust Global Root CA R2	Root Key	sha384ECDSA	384 bits	E45366B7B7A4E9D7CCC121E04ACFCCAC01BC72BC	78919B35D1C615595A51328A5C546083B4D5320724A258695B991F2F61C4DCC7	UniTrust Global Root CA R2
SHECA DV Server CA 2A	Signing Key	sha384ECDSA	384 bits	A1221170BEC8665F6ECB104C4EDB38EA9C1F914D	69201DC24E4127FFA5B41A0DDF0A1A005C00F334B003F1008924CBF998E1827C	UniTrust Global Root CA R2
SHECA OV Server CA 2A	Signing Key	sha384ECDSA	384 bits	98CDEC338767F39422373810B735BA7C683A8259	8E2CA2825C2039804A7A1CC54B002EA1DB30AC489698F039527BF1602132F611	UniTrust Global Root CA R2
SHECA EV Server CA 2A	Signing Key	sha384ECDSA	384 bits	44661C71EF69B7930AB5B771D83B114CFA843D77	93E49170D20F54DA701118A5ABDCDDA4FFCF334CDB2D8D80599AB62848C85F80	UniTrust Global Root CA R2

上海市数字证书认证中心有限公司

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

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

2022 年 4 月 22 日

致：普华永道中天会计师事务所（特殊普通合伙）

就 2021 年 5 月 1 日到 2022 年 3 月 31 日期间 SSL 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，并遵循 SSL 基准规范与网络安全服务提供 SSL 电子认证服务，附件列示了服务所包括的根证书和中级证书。

SHECA 管理层已对证书业务披露和 SSL 电子认证服务控制进行评估。基于此评估，在 2021 年 5 月 1 日至 2022 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 电子认证服务期间，SHECA：

- 披露SSL证书生命周期管理业务规则于：
  - UniTrust证书认证业务规则 v3.7.1 (https://assets-cdn.sheca.com/documents/SHECA-CPS-v3.7.1%EF%BC%88EN%EF%BC%89.pdf);
  - UniTrust证书认证业务规则 v3.7；
  - UniTrust证书认证业务规则 v3.6.9；以及
  - UniTrust证书策略 v1.4.9 (https://assets-cdn.sheca.com/documents/SHECA-CP-v1.4.9%20%EF%BC%88EN%20).pdf);
  - UniTrust证书策略 v1.4.8；
  - UniTrust证书策略 v1.4.7.

  包括承诺遵循CAB论坛（CA/Browser Forum）的相关指引提供SSL电子认证服务，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证书在生命周期中的完整性；以及
  - 恰当地鉴证（SHECA所执行的注册操作）SSL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的授权和执行，以维持CA系统的完整。

- 通过有效控制机制，以提供合理保证确保符合CAB论坛（CA/Browser Forum）发布的网络及证书系统安全规范（Network and Certificate System Security Requirements）。

以符合 WebTrust 电子认证 SSL 基准规范与网络安全规范审计标准 v2.5 （WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security v2.5）（https://www.cpacanada.ca/-/media/site/operational/ms-member-services/docs/webtrust/wt100bwtbr-25-110120-finalaoda.pdf?la=en&hash=11A5FE85CBF7F0E960E681DFF6FD4592FC135B4C）。

_____

崔久强
上海市数字证书认证中心有限公司总经理

_____

公司盖章

附件

下表列示本认定报告所包括的密钥和证书：

密钥名称	密钥种类	密钥算法	密钥长度	密钥 ID	证书指纹（SHA256）	证书签发者
UCA Global G2 Root	Root Key	sha256RSA	4096 bits	81C48CCCF5E430F FA50C085F8C1567 217401DFDF	9BEA11C976FE014764 C1BE56A6F914B5A560 317ABD9988393382E5 161AA0493C	UCA Global G2 Root
UCA Global G2 Root	Root Key	sha256RSA	4096 bits	81C48CCCF5E430F FA50C085F8C1567 217401DFDF	C1AFC65B1E813B0E61 46E6AA5341681272AB E9A38D59F7BD1B27B 729834A0D9C	Certum Trusted Network CA
SHECA RSA Domain Validation Server CA G3	Signing Key	sha256RSA	2048 bits	057A4D756FFD0A 83B1671675773E14 C5F53C548E	0A552A65F22FF820E7 EC3D43BBF88B02ABC 34BD247E0C3505891B 6342F16A5F2	UCA Global G2 Root
SHECA RSA Organization Validation Server CA G3	Signing Key	sha256RSA	2048 bits	316068091E32F9F 6CCC06215AA7B91 AF4C119D40	26FD4C4367E463D39 C71796AE4010E53380 DC93BC132FB019D671 8A6873E81F4	UCA Global G2 Root
SHECA DV Server CA G5	Signing Key	sha256RSA	2048 bits	D8E7061B645FAB3 008887A2453AAE1 1C8304BF6D	778C516DAEC700EE5 8B3581E411E5C0DD47 8663A5163A298953415 07D6E964DD	UCA Global G2 Root
SHECA OV Server CA G5	Signing Key	sha256RSA	2048 bits	0379A38D525FD4 E988921F4358542 502F4878B7E	8AB3A0ACF289E6EF7 54BE449236843D67F4 5C191BDDD66484B85 E6E60556A9AF	UCA Global G2 Root
SHECA EV Server CA G2	Signing Key	sha256RSA	2048 bits	86B148C0420A9C6 F81FC4FDCD10F18 4BAAB5A6EA	4216527163AD2CAA82 5D3BF48F61A7661D0A BC89B58AB76B23A1E1 0999F0769F	UCA Global G2 Root
TrustAsia RSA DV TLS CA - S1	Signing Key	sha256RSA	2048 bits	9432E0D48ACD1D 93E75C5372960C5 EF1F3F67972	074ADD7F1E73EB110E C8E2B78A92C51CF5A4 51135B6F7DEFC019EE 9D74BFA4D6	UCA Global G2 Root
TrustAsia RSA OV TLS CA - S1	Signing Key	sha256RSA	2048 bits	F575D48E293E17A 8A9C49EDCE6DB0 A344D132AEB	D16BA9ACB74FEE4AA 8087EE482E86E7F6F5 F55FAC502563973075 3FE1E705E3C	UCA Global G2 Root
UCA Extended Validation Root	Root Key	sha256RSA	4096 bits	D9743AE4303D0D F712DC7E5A059F1 E349AF7E114	D43AF9B35473755C96 84FC06D7D8CB70EE5 C28E773FB294EB41EE 71722924D24	UCA Extended Validation Root
SHECA RSA Extended Validation Server CA	Signing Key	sha256RSA	2048 bits	3B4B252A77372AF CB97FEDA8BDAF2 299FC5DC5F4	4FD6FA527157EEA463 689D7A4C2B934EF22 2279725413893D98472 42C85CA9DF	UCA Extended Validation Root
SHECA EV Server CA G3	Signing Key	sha256RSA	2048 bits	54E972FB78669FE 5CBF33B8F984655 53739C0B84	7EF3F89456CE636557 B20C5DFB37F98C253 A0B660D2E9E5E7845 CAF9C038C7C1	UCA Extended Validation Root
UniTrust Global Root CA R1	Root Key	sha384RSA	4096 bits	3CA061B0EFDAC6 E8BB2DE156A2EB BBB63D232381	81B35EFC42C7794720 9D76B51B5E7B122CE7 8348AE8C4525DC8D4 B30289E5385	UniTrust Global Root CA R1

密钥名称	密钥种类	密钥算法	密钥长度	密钥 ID	证书指纹（SHA256）	证书签发者
SHECA DV Server CA 1A	Signing Key	sha384RSA	4096 bits	653740E0BBF43905206A8C9CA0ACB3BBD6968CA0	D3D4A040BB41A695A96E3AAD93814CF7EF219D5819206E947B44DCC5B8E5E272	UniTrust Global Root CA R1
SHECA OV Server CA 1A	Signing Key	sha384RSA	4096 bits	8CD02E82008EE2DEFF71F61A105C74A826E858D1	9A3DB0F0FB0FF4F974A4E0C510A7C13D350485B1E6CDF5A899BB24D0F499E9BD	UniTrust Global Root CA R1
SHECA EV Server CA 1A	Signing Key	sha384RSA	4096 bits	73E36DF62D862F57DF69A53687231C85E0170216	2F1CA1A5C0D7AE58C7ADFC69D4C57EE815F39C0F3D1F982E3AC76D25AB723995	UniTrust Global Root CA R1
UniTrust Global Root CA R2	Root Key	sha384ECDSA	384 bits	E45366B7B7A4E9D7CCC121E04ACFCCAC01BC72BC	78919B35D1C615595A51328A5C546083B4D5320724A258695B991F2F61C4DCC7	UniTrust Global Root CA R2
SHECA DV Server CA 2A	Signing Key	sha384ECDSA	384 bits	A1221170BEC8665F6ECB104C4EDB38EA9C1F914D	69201DC24E4127FFA5B41A0DDF0A1A005C00F334B003F1008924CBF998E1827C	UniTrust Global Root CA R2
SHECA OV Server CA 2A	Signing Key	sha384ECDSA	384 bits	98CDEC338767F3942237381OB735BA7C683A8259	8E2CA2825C2039804A7A1CC54B002EA1DB30AC489698F039527BF1602132F611	UniTrust Global Root CA R2
SHECA EV Server CA 2A	Signing Key	sha384ECDSA	384 bits	44661C71EF69B7930AB5B771D83B114CFA843D77	93E49170D20F54DA701118A5ABDCDDA4FFCF334CDB2D8D80599AB62848C85F80	UniTrust Global Root CA R2