INDEPENDENT PRACTITIONER'S ASSURANCE REPORT

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

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

Management's Responsibilities

SHECA's management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities 2.2.

Our Independence and Quality Control

We have complied with the independence and other ethical requirement of the International Code of Ethics for Professional Accountants (including International Independence Standards) issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

Our firm applies International Standard on Quality Control 1 and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Practitioner's Responsibilities

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

We conducted our work in accordance with the International Standard on Assurance Engagements 3000 (Revised) "Assurance Engagements Other Than Audits or Reviews of Historical Financial Information". This standard requires that we plan and perform our work to form the opinion.

A reasonable assurance engagement involves performing procedures to obtain sufficient appropriate evidence whether the management assertion of SHECA is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities 2.2. 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 key and

INDEPENDENT PRACTITIONER'S ASSURANCE REPORT (CONTINUED)

certificate lifecycle management business practices and its controls over key and certificate integrity, over the authenticity and confidentiality of subscriber and relying party information, over the continuity of key and certificate lifecycle management operations and over development, maintenance and operation of systems integrity; (2) selectively testing transactions executed in accordance with disclosed key and 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.

SHECA makes use of external registration authorities for specific subscriber registration activities as disclosed in SHECA's business practices. Our procedures did not extend to the controls exercised by these external registration authorities.

The relative effectiveness and significance of specific controls at SHECA and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Inherent Limitation

We draw attention to the fact that the WebTrust Principles and Criteria for Certification Authorities 2.2 includes certain inherent limitations that can influence the reliability of the information.

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

Opinion

In our opinion, the accompanying assertion of SHECA, for the period from May 1, 2019 to April 30, 2020, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities 2.2.

Emphasis of Matter

Without modifying our conclusion, we draw attention to the fact that this report does not include any representation as to the quality of SHECA's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities 2.2, nor the suitability of any of SHECA's services for any customer's intended purpose.

INDEPENDENT PRACTITIONER'S ASSURANCE REPORT (CONTINUED)

Other Matter

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

Purpose and Restriction on Use

The accompanying assertion was prepared for obtaining and displaying the WebTrust Seal on SHECA website[1] using the WebTrust Principle and Criteria for Certification Authorities 2.2 designed for this purpose. As a result, the accompanying assertion of SHECA may not be suitable for another purpose. This report is intended solely for the Management of SHECA in connection with obtaining and displaying the WebTrust Seal on its website for submission of the report to the related authority in connection with the WebTrust Principle and Criteria for Certification Authorities 2.2. We do not assume responsibility towards or accept liability to any other person for the contents of this report.

PricewaterhouseCoopers
Certified Public Accountants

Hong Kong, China

June 12, 2020

[1] *The maintenance and integrity of the SHECA website is the responsibility of the directors; the work carried out by the assurance provider does not involve consideration of these matters and, accordingly, the assurance provider accepts no responsiblity for any differences between the accompanying assertion by the management of SHECA on which the assurance report was issued or the assurance report that was issued and the information presented on the website.*

注册会计师独立鉴证报告
（注意：本中文报告只作参考。正文请参阅英文报告。）

致：上海市数字证书认证中心有限公司管理层

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

管理层的责任

SHECA的管理层负责确保管理层认定，包括其陈述的客观性以及认定中描述的SHECA所提供的服务能够符合WebTrust电子认证资格原则及规范V2.2的规定。

我们的独立性和质量控制

我们遵守了国际会计师职业道德准则理事会颁布的国际会计师道德守则（包括国际独立性标准）中的独立性及其他职业道德要求。该职业道德守则以诚信、客观、专业胜任能力及应有的关注、保密和良好职业行为为基本原则。

本事务所遵循国际质量控制准则第 1 号，据此维护全面系统的质量控制体系，包括与遵守职业道德要求、专业标准和适用的法律和法规要求的书面政策与程序。

注册会计师的责任

我们的责任是在执行鉴证工作的基础上对管理层认定发表意见。

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

合理保证的鉴证业务涉及实施鉴证程序，以获取有关管理层认定是否在所有重大方面符合 WebTrust 电子认证资格原则及规范 V2.2 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 密钥和证书生命周期管理及对密钥和证书完整性的控制措施，包括订户和依赖方信息的真实性和保密性，密钥和证书生命周期管理的连续性，以及系统开发、运维的完整性；（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遵守所披露的业务规则委托外部用户注册机构（External Registration Authorities）对个别用户进行用户信息鉴定工作。我们的鉴证程序并不伸延至这些外部用户注册机构所实施的控制措施。

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

我们提请使用者注意，WebTrust 电子认证资格原则及规范 V2.2 具有某些可能影响鉴证对象信息可靠性的固有限制。

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

意见

我们认为，SHECA 于 2019 年 5 月 1 日至 2020 年 4 月 30 日期间的电子认证服务的管理层认定在所有重大方面符合 WebTrust 电子认证资格原则及规范 V2.2。

强调事项

我们提请使用者关注，本报告并不包括任何在 WebTrust 电子认证资格原则及规范 V2.2 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

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。

目的及使用限制

后附管理层认定为在 SHECA 网站 [1]上获取并展示 WebTrust Seal 编制，并采用为该目的而设计的 WebTrust 电子认证资格原则及规范 V2.2，因此后附 SHECA 管理层认定可能不适用于其他目的。本报告仅供 SHECA 管理层根据 WebTrust 电子认证资格原则及规范 V2.2，持续获得并在 SHECA 网站上展示 WebTrust 电子认证标识而向 WebTrust 相关机构（CPA Canada）提交的目的使用。我们不会就本报告的内容向任何其他人士负上或承担任何责任。

---

[1] SHECA 网站维护和网站的真实完整是公司董事的职责。我们执行的鉴证程序不包含对该等事项的考虑，因此，对出具本鉴证报告所依赖的 SHECA 管理层认定或鉴证报告与网站所显示信息的任何差异我们均不承担责任。

注册会计师独立鉴证报告（续）

罗兵咸永道会计师事务所
执业会计师

香港，2020年6月12日

Shanghai Electronic Certificate Authority Center Co.,Ltd

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

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

June 12, 2020

Dear Sirs,

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

Shanghai Electronic Certificate Authority Center Co., Ltd. ("SHECA") operates the Certification Authority (CA) services known as its Root and Subordinate CAs (please refer to the appendix), and provides the following CA services:

- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation
- Subscriber key generation and management
- Subordinate CA certification

The management of SHECA is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure on its website, CA business practices management, CA environmental controls, CA key lifecycle management controls, subscriber key lifecycle management controls, certificate lifecycle management controls, and subordinate CA 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 CA services. Based on that assessment, in SHECA management's opinion, in providing its Certification Authority (CA) services at Shanghai, China, throughout the period May 1, 2019 to Aril 30, 2020, SHECA has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environment control practices in its:
  - UniTrust Certification Practice Statement Version 3.6.6 (https://assets-cdn.sheca.com/documents/sheca-certification-practice-statement-en-v3.6.6.pdf) ;
  - UniTrust Certification Practice Statement Version 3.6.5;
  - UniTrust Certification Practice Statement Version 3.6.4;
  - UniTrust Certification Practice Statement Version 3.6.3;
  - UniTrust Certificate Policy Version 1.4.4 (https://assets-cdn.sheca.com/documents/unitrust-certificate-policy-en-v1.4.4.pdf);
  - UniTrust Certificate Policy Version 1.4.3;
  - UniTrust Certificate Policy Version 1.4.2;
  - UniTrust Certificate Policy Version 1.4.1; and
  - UniTrust Event Certification Policy & Certification Practice Statement v1.1 (https://assets-cdn.sheca.com/documents/unitrust-event-certificate-policy-certification-practice-statement-en-v1.1.pdf);
  - UniTrust Event Certification Policy & Certification Practice Statement v1.0,

- maintained effective controls to provide reasonable assurance that:
  - SHECA's Certification Practice Statement is consistent with its Certificate Policy
  - SHECA provides its services in accordance with its Certification Practice Statements

- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
  - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles;
  - subscriber information is properly authenticated (for the registration activities performed by SHECA); and
  - subordinate CA certificate requests are accurate, authenticated, and approved

- 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 2.2 (https://www.cpacanada.ca/-/media/site/operational/ms-member-services/docs/webtrust/webtrust-for-ca-22.pdf?la=en&hash=F377F94E2E3D87A83D07DDAC54171AC01AE798FA), including the following:

CA Business Practices Disclosure

- Certification Practice Statement (CPS)
- Certificate Policy (CP)

CA Business Practices Management

- Certificate Policy Management
- Certification Practice Statement Management
- CP and CPS Consistency

CA Environmental Controls

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical & Environmental Security
- Operations Management
- System Access Management
- System Development and Maintenance
- Business Continuity Management
- Monitoring and Compliance
- Audit Logging

CA Key Lifecycle Management Controls

- CA Key Generation
- CA Key Storage, Backup, and Recovery
- CA Public Key Distribution
- CA Key Usage
- CA Key Archival and Destruction
- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management

Subscriber Key Lifecycle Management Controls

- CA-Provided Subscriber Key Generation Services
- CA-Provided Subscriber Key Storage and Recovery Services
- Integrated Circuit Card (ICC) Lifecycle Management
- Requirements for Subscriber Key Management

Certificate Lifecycle Management Controls

- Subscriber Registration
- Certificate Renewal
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Validation

Subordinate CA Certificate Lifecycle Management Controls

- Subordinate CA Certificate Lifecycle Management

SHECA does not escrow its CA keys, and does not provide certificate suspension services. Accordingly, our assertion does not extend to controls that would address those criteria.

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

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 Key Identifier	Certificates (Thumbprint)	Certificate Signed by
UCA Root G2	Root Key	sha256RSA	2048 bits	e4 bb 2c 9f b2 b5 1c 88 31 af 7f cb dc f4 05 2b e0 85 f7 01	A07919A6391BCD6E15FB33A41B43A938EF3D19CF54F0198EC29D02364BC5A0EC	UCA Root G2
SHECA G2	Signing Key	sha256RSA	2048 bits	56 88 de e3 18 43 82 b7 72 a4 26 eb 44 a9 62 d0 87 c4 ac 26	69275DE8AF892E26E1B5339A664C194550799372F13CA6FB4966408F6A43C5B4	UCA Root G2
GlobalSign China CA for AATL	Signing Key	sha256RSA	2048 bits	fc ad 8a ad bf 32 3a ff 97 c0 9b d7 4a 70 39 88 89 19 d4 6a	D883436D97B08B008810D2EF3852D322E1D3528C751D3B23FF0C80803ED1CFAE	UCA Root G2
UCA Root SM2	Root Key	SM2	256 bits	ee e8 b0 9c d5 dc ec 73 fd ef 7c fa 50 2c c6 c1 40 e6 4c b3	307C77562B1532AE5FA6E63ED597CD54A0CBCC111F3598A7CCB2E19DD1351362	UCA Root SM2
UniTrust DV Secure Server CA G4	Signing Key	SM2	256 bits	ad a6 11 69 60 54 f8 98 ce d2 69 54 2a 29 df 23 94 84 e8 33	68B5E5FCA21925C5AF6628341FE6DBD187C6E66AEEF5F58295DCD7238FF56AD8	UCA Root SM2
UniTrust OV Secure Server CA G4	Signing Key	SM2	256 bits	d6 54 6f a6 58 72 75 42 0b f2 04 79 4c 4c 6d e4 36 8a 8b d5	E75A9D14B5C5FF14779F0DC8A7889EE757788DC82706D95B4E2AF039098FA72C	UCA Root SM2
SHECA SM2	Signing Key	SM2	256 bits	89 31 04 91 7b 43 aa aa 9a bf 84 1d 9b 86 ee f0 b8 70 99 a0	F5F6192276AED2141B3A66FD66724D46C5A58CACF618CAA5B5AA546ED5865207	UCA Root SM2
UCA Global G2 Root	Root Key	sha256RSA	4096 bits	81 c4 8c cc f5 e4 30 ff a5 0c 08 5f 8c 15 67 21 74 01 df df	9BEA11C976FE014764C1BE56A6F914B5A560317ABD9988393382E5161AA0493C	UCA Global G2 Root
UCA Global G2 Root	Root Key	sha256RSA	4096 bits	81 c4 8c cc f5 e4 30 ff a5 0c 08 5f 8c 15 67 21 74 01 df df	C1AFC65B1E813B0E6146E6AA5341681272ABE9A38D59F7BD1B27B729834A0D9C	Certum Trusted Network CA
SHECA Global G3 SSL	Signing Key	sha256RSA	2048 bits	98 20 f0 f1 d9 42 a6 de 83 3f 99 10 19 00 3d 68 68 d2 01 81	AEFFE4335EE56422E927F45E95AE142B9EB35979A7400569AE9BDEA6CAABC1DC	UCA Global G2 Root
SHECA Global G3 Code Signing	Signing Key	sha256RSA	2048 bits	f7 3d f9 39 a8 d9 87 54 ac 77 8e f5 d9 95 ee f8 35 ab 94 39	EAA5AD8E9A2FA992354B2FF4254BEB08A632F7F17602604DDED58D73D616D844	UCA Global G2 Root

Key Name	Key Type	Signature Algorithm	Key Size	Subject Key Identifier	Certificates (Thumbprint)	Certificate Signed by
SHECA RSA Code Signing CA G3	Signing Key	sha256RSA	2048 bits	fd 7e c8 7a c2 77 1c 56 87 d2 ae f8 07 c7 42 6a 1b 7c 42 a8	C7E976AA77E92491C269840B2F1461E65147A2BB181EE59AB63BCD86704FE456	UCA Global G2 Root
SHECA RSA Domain Validation Server CA G3	Signing Key	sha256RSA	2048 bits	05 7a 4d 75 6f fd 0a 83 b1 67 16 75 77 3e 14 c5 f5 3c 54 8e	0A552A65F22FF820E7EC3D43BBF88B02ABC34BD247E0C3505891B6342F16A5F2	UCA Global G2 Root
SHECA RSA Organization Validation Server CA G3	Signing Key	sha256RSA	2048 bits	31 60 68 09 1e 32 f9 f6 cc c0 62 15 aa 7b 91 af 4c 11 9d 40	26FD4C4367E463D39C71796AE4010E53380DC93BC132FB019D6718A6873E81F4	UCA Global G2 Root
SHECA RSA Time Stamp Authority G1	Signing Key	sha256RSA	2048 bits	6f c5 77 0c 4e 82 5e 4b 54 4b 30 bd 99 33 f4 08 57 1a 3d b4	86EE4A2F93137CA8887674078B394070F189B3049DD2D24053AE92924254C668	UCA Global G2 Root
UCA Extended Validation Root	Root Key	sha256RSA	4096 bits	d9 74 3a e4 30 3d 0d f7 12 dc 7e 5a 05 9f 1e 34 9a f7 e1 14	D43AF9B35473755C9684FC06D7D8CB70EE5C28E773FB294EB41EE71722924D24	UCA Extended Validation Root
SHECA Extended Validation SSL CA	Signing Key	sha256RSA	2048 bits	4d 14 0d ea 6b 55 9c 0c a6 e1 bb 7b e8 6a 96 6d 17 5e 7c b5	25BFDB1C5FE2CCE051EC6DFBF2BB24E78C92F969B1BB37867DAEDF93D1A7AE7E	UCA Extended Validation Root
SHECA Extended Validation Code Signing CA	Signing Key	sha256RSA	2048 bits	74 98 99 6f 6a 15 c0 06 25 20 85 1c af 2b 31 6b 87 ed a3 db	A392C645B9A5AD6A214F19DE776346BC7DD6BB15818E433886DAC54EE6661852	UCA Extended Validation Root
SHECA RSA Extended Validation Server CA	Signing Key	sha256RSA	2048 bits	3b 4b 25 2a 77 37 2a fc b9 7f ed a8 bd af 22 99 fc 5d c5 f4	4FD6FA527157EEA463689D7A4C2B934EF2222797254138 93D9847242C85CA9DF	UCA Extended Validation Root
SHECA RSA Extended Validation Code Signing CA	Signing Key	sha256RSA	2048 bits	8e 40 66 5f 6a a9 40 c2 b9 f1 f0 4a 22 63 95 64 59 37 07 e5	D404FAFA4BA2F426B66CD219C6DA84F91C0FB7CB58429EC8077E2A764314D55D	UCA Extended Validation Root
UniTrust Event Certificate Root CA R1	Root Key	sha384RSA	4096 bits	d7 41 8b ee d4 5f c6 e9 7d 69 10 86 08 ac 7e e4 8b a0 72 7e	3200B1BC5CF8F8BC0A382BD7809166A221600747DEC386D2625959CD75A28212	UniTrust Event Certificate Root CA R1
SHECA Event Certificate CA G1	Signing Key	sha256RSA	2048 bits	2a 4d 75 75 34 7f ff b4 6a 57 51 38 16 ff a9 9e ea af 0f 4f	32AE6837AEF2DABBC8C19385A57A19FC97F6BDB8384B1ADCCDEAED3A891A3A0F	UniTrust Event Certificate Root CA R1
UniTrust Global Root CA R1	Root Key	sha384RSA	4096 bits	3c a0 61 b0 ef da c6 e8 bb 2d e1 56 a2 eb bb b6 3d 23 23 81	81B35EFC42C77947209D76B51B5E7B122CE78348AE8C4525DC8D4B30289E5385	UniTrust Global Root CA R1

Key Name	Key Type	Signature Algorithm	Key Size	Subject Key Identifier	Certificates (Thumbprint)	Certificate Signed by
UniTrust Global Root CA R2	Root Key	sha384ECDSA	384 bits	e4 53 66 b7 b7 a4 e9 d7 cc c1 21 e0 4a cf cc ac 01 bc 72 bc	78919B35D1C615595A51328A5C546083B4D5320724A258695B991F2F61C4DCC7	UniTrust Global Root CA R2
UniTrust Global Root CA R3	Root Key	SM2	256 bits	3b 15 e6 2b 1c 9f 50 15 b6 4e a1 6d 16 3a 55 8a f4 90 5f b5	6A19BCC7FAD2A5664F779BF143A72A2B079AC476E56FACBA48C352635CB4718F	UniTrust Global Root CA R3

上海市数字证书认证中心有限公司

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

罗兵咸永道会计师事务所
中国香港
中环太子大厦22楼

2020 年 6 月 12 日

致：罗兵咸永道会计师事务所

就 2019 年 5 月 1 日到 2020 年 4 月 30 日期间电子认证业务规则披露和电子认证运行控制活动的管理层认定报告
（本中文报告只作参考，正文请参阅英文报告。）

上海市数字证书认证中心有限公司（Shanghai Electronic Certificate Authority Center Co., Ltd.，简称“SHECA”）运营电子认证服务机构（附件列示了服务所包括的根证书和中级证书），并提供以下电子认证（以下简称“CA”）服务：

- 订户注册
- 证书更新
- 证书密钥更新
- 证书签发
- 证书分发
- 证书撤销
- 证书验证
- 订户密钥生成和管理
- 下级CA认证

SHECA 的管理层负责针对 CA 服务建立并维护有效的控制，包括：CA 业务规则披露，CA 业务规则管理，CA 环境控制，CA 密钥生命周期管理，订户密钥生命周期管理，证书生命周期管理，以及下级 CA 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 管理层已对所提供的电子认证服务的业务规则披露及控制进行评估。基于此评估，SHECA 管理层认为，在 2019 年 5 月 1 日至 2020 年 4 月 30 日就 SHECA 在中国上海所提供的电子认证服务期间，SHECA：

- 披露电子认证业务、密钥生命周期管理、证书生命周期管理，以及CA环境控制管理

于：

- UniTrust 证书策略 v1.4.4（https://assets-cdn.sheca.com/documents/unitrust-certificate-policy-cn-v1.4.4.pdf）；
- UniTrust 证书策略 v1.4.3；
- UniTrust 证书策略 v1.4.2；
- UniTrust 证书策略 v1.4.1；
- UniTrust证书认证业务规则 v3.6.6（https://assets-cdn.sheca.com/documents/sheca-certification-practice-statement-cn-v3.6.6.pdf）；
- UniTrust证书认证业务规则 v3.6.5；
- UniTrust证书认证业务规则 v3.6.4；
- UniTrust证书认证业务规则 v3.6.3；以及
- UniTrust事件证书证书策略 & 认证业务规则 v1.1（https://assets-cdn.sheca.com/documents/unitrust-event-certificate-policy-certification-practice-statement-cn-v1.1.pdf）；
- UniTrust事件证书证书策略 & 认证业务规则 v1.0。

- 通过有效控制机制，以提供以下合理保证：
  - SHECA的CPS与CP相符；
  - SHECA遵循CP和CPS提供电子认证服务。

- 通过有效控制机制，以提供以下合理保证：
  - 有效维护所管理的密钥与证书在生命周期中的完整性；
  - 建立并保护所管理的订户密钥和订户证书在生命周期中的完整性；
  - 恰当地鉴证（SHECA所执行的注册操作）订户证书申请者的信息；以及
  - 下级CA证书请求是准确、经鉴证并通过批准的。

- 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。

以符合 WebTrust 电子认证审计标准 V2.2（WebTrust Principles and Criteria for Certification Authorities 2.2）（https://www.cpacanada.ca/-/media/site/operational/ms-member-services/docs/webtrust/webtrust-for-ca-22.pdf?la=en&hash=F377F94E2E3D87A83D07DDAC54171AC01AE798FA），包括以下内容：

CA业务规则披露

- 电子认证业务规则（CPS）
- 证书策略（CP）

CA业务规则管理

- 证书策略管理
- 电子认证业务规则管理
- CP和CPS的一致性

CA环境控制

- 安全管理

- 资产分类与管理
- 人员安全
- 物理及环境安全
- 运营管理
- 系统访问管理
- 系统开发与维护管理
- 业务持续性管理
- 监控与合规管理
- 审计日志管理

CA密钥生命周期管理

- CA密钥生成
- CA密钥保管、备份及恢复
- CA公钥分发
- CA密钥用途
- CA密钥归档和销毁
- CA密钥泄露
- CA加密设备生命周期管理

订户密钥生命周期管理

- CA提供的订户密钥生成服务
- CA提供的订户密钥保管及恢复服务
- IC卡生命周期管理
- 对订户密钥管理的要求

电子证书生命周期管理

- 订户注册
- 证书更新
- 证书密钥更新
- 证书签发
- 证书分发
- 证书撤销
- 证书验证

下级CA证书生命周期管理

- 下级CA证书生命周期管理

SHECA 不托管其 CA 密钥，并且不提供证书挂起服务。因此，我们的报告范围不会覆盖到这些控制点。

崔久强
上海市数字证书认证中心有限公司总经理

_____

公司盖章

附件

下表列示本认定报告所包括的密钥和证书：

密钥名称	密钥种类	密钥算法	密钥长度	密钥 ID	证书指纹	证书签发者
UCA Root G2	Root Key	sha256RSA	2048 bits	e4 bb 2c 9f b2 b5 1c 88 31 af 7f cb dc f4 05 2b e0 85 f7 01	A07919A6391BCD6E15FB33A41B43A938EF3D19CF54F0198EC29D02364BC5A0EC	UCA Root G2
SHECA G2	Signing Key	sha256RSA	2048 bits	56 88 de e3 18 43 82 b7 72 a4 26 eb 44 a9 62 d0 87 c4 ac 26	69275DE8AF892E26E1B5339A664C194550799372F13CA6FB4966408F6A43C5B4	UCA Root G2
GlobalSign China CA for AATL	Signing Key	sha256RSA	2048 bits	fc ad 8a ad bf 32 3a ff 97 c0 9b d7 4a 70 39 88 89 19 d4 6a	D883436D97B08B008810D2EF3852D322E1D3528C751D3B23FF0C80803ED1CFAE	UCA Root G2
UCA Root SM2	Root Key	SM2	256 bits	ee e8 b0 9c d5 dc ec 73 fd ef 7c fa 50 2c c6 c1 40 e6 4c b3	307C77562B1532AE5FA6E63ED597CD54A0CBCC111F3598A7CCB2E19DD1351362	UCA Root SM2
UniTrust DV Secure Server CA G4	Signing Key	SM2	256 bits	ad a6 11 69 60 54 f8 98 ce d2 69 54 2a 29 df 23 94 84 e8 33	68B5E5FCA21925C5AF6628341FE6DBD187C6E66AEEF5F58295DCD7238FF56AD8	UCA Root SM2
UniTrust OV Secure Server CA G4	Signing Key	SM2	256 bits	d6 54 6f a6 58 72 75 42 0b f2 04 79 4c 4c 6d e4 36 8a 8b d5	E75A9D14B5C5FF14779F0DC8A7889EE757788DC82706D95B4E2AF039098FA72C	UCA Root SM2
SHECA SM2	Signing Key	SM2	256 bits	89 31 04 91 7b 43 aa aa 9a bf 84 1d 9b 86 ee f0 b8 70 99 a0	F5F6192276AED2141B3A66FD66724D46C5A58CACF618CAA5B5AA546ED5865207	UCA Root SM2

密钥名称	密钥种类	密钥算法	密钥长度	密钥 ID	证书指纹	证书签发者
UCA Global G2 Root	Root Key	sha256RSA	4096 bits	81 c4 8c cc f5 e4 30 ff a5 0c 08 5f 8c 15 67 21 74 01 df df	9BEA11C976FE014764C1BE56A6F914B5A560317ABD9988393382E5161AA0493C	UCA Global G2 Root
UCA Global G2 Root	Root Key	sha256RSA	4096 bits	81 c4 8c cc f5 e4 30 ff a5 0c 08 5f 8c 15 67 21 74 01 df df	C1AFC65B1E813B0E6146E6AA5341681272ABE9A38D59F7BD1B27B729834A0D9C	Certum Trusted Network CA
SHECA Global G3 SSL	Signing Key	sha256RSA	2048 bits	98 20 f0 f1 d9 42 a6 de 83 3f 99 10 19 00 3d 68 68 d2 01 81	AEFFE4335EE56422E927F45E95AE142B9EB35979A7400569AE9BDEA6CAABC1DC	UCA Global G2 Root
SHECA Global G3 Code Signing	Signing Key	sha256RSA	2048 bits	f7 3d f9 39 a8 d9 87 54 ac 77 8e f5 d9 95 ee f8 35 ab 94 39	EAA5AD8E9A2FA992354B2FF4254BEB08A632F7F17602604DDED58D73D616D844	UCA Global G2 Root
SHECA RSA Code Signing CA G3	Signing Key	sha256RSA	2048 bits	fd 7e c8 7a c2 77 1c 56 87 d2 ae f8 07 c7 42 6a 1b 7c 42 a8	C7E976AA77E92491C269840B2F1461E65147A2BB181EE59AB63BCD86704FE456	UCA Global G2 Root
SHECA RSA Domain Validation Server CA G3	Signing Key	sha256RSA	2048 bits	05 7a 4d 75 6f fd 0a 83 b1 67 16 75 77 3e 14 c5 f5 3c 54 8e	0A552A65F22FF820E7EC3D43BBF88B02ABC34BD247E0C3505891B6342F16A5F2	UCA Global G2 Root
SHECA RSA Organization Validation Server CA G3	Signing Key	sha256RSA	2048 bits	31 60 68 09 1e 32 f9 f6 cc c0 62 15 aa 7b 91 af 4c 11 9d 40	26FD4C4367E463D39C71796AE4010E53380DC93BC132FB019D6718A6873E81F4	UCA Global G2 Root
SHECA RSA Time Stamp Authority G1	Signing Key	sha256RSA	2048 bits	6f c5 77 0c 4e 82 5e 4b 54 4b 30 bd 99 33 f4 08 57 1a 3d b4	86EE4A2F93137CA8887674078B394070F189B3049DD2D24053AE92924254C668	UCA Global G2 Root
UCA Extended Validation Root	Root Key	sha256RSA	4096 bits	d9 74 3a e4 30 3d 0d f7 12 dc 7e 5a 05 9f 1e 34 9a f7 e1 14	D43AF9B35473755C9684FC06D7D8CB70EE5C28E773FB294EB41EE71722924D24	UCA Extended Validation Root
SHECA Extended Validation SSL CA	Signing Key	sha256RSA	2048 bits	4d 14 0d ea 6b 55 9c 0c a6 e1 bb 7b e8 6a 96 6d 17 5e 7c b5	25 BF DB 1C 5F E2 CC E0 51 EC 6D FB F2 BB 24 E7 8C 92 F9 69 B1 BB 37 86 7D AE DF 93 D1 A7 AE 7E	UCA Extended Validation Root
SHECA Extended Validation Code Signing CA	Signing Key	sha256RSA	2048 bits	74 98 99 6f 6a 15 c0 06 25 20 85 1c af 2b 31 6b 87 ed a3 db	A3 92 C6 45 B9 A5 AD 6A 21 4F 19 DE 77 63 46 BC 7D D6 BB 15 81 8E 43 38 86 DA C5 4E E6 66 18 52	UCA Extended Validation Root

密钥名称	密钥种类	密钥算法	密钥长度	密钥 ID	证书指纹	证书签发者
SHECA RSA Extended Validation Server CA	Signing Key	sha256RSA	2048 bits	3b 4b 25 2a 77 37 2a fc b9 7f ed a8 bd af 22 99 fc 5d c5 f4	4FD6FA527157EEA463689D7A4C2B934EF2222797254138 93D9847242C85CA9DF	UCA Extended Validation Root
SHECA RSA Extended Validation Code Signing CA	Signing Key	sha256RSA	2048 bits	8e 40 66 5f 6a a9 40 c2 b9 f1 fo 4a 22 63 95 64 59 37 07 e5	D404FAFA4BA2F4 26B66CD219C6DA 84F91C0FB7CB584 29EC8077E2A7643 14D55D	UCA Extended Validation Root
UniTrust Event Certificate Root CA R1	Root Key	sha384RSA	4096 bits	d7 41 8b ee d4 5f c6 e9 7d 69 10 86 08 ac 7e e4 8b a0 72 7e	3200B1BC5CF8F8B C0A382BD7809166 A221600747DEC38 6D2625959CD75A2 8212	UniTrust Event Certificate Root CA R1
SHECA Event Certificate CA G1	Signing Key	sha256RSA	2048 bits	2a 4d 75 75 34 7f ff b4 6a 57 51 38 16 ff a9 9e ea af 0f 4f	32AE6837AEF2DA BBC8C19385A57A1 9FC97F6BDB8384 B1ADCCDEAED3A 891A3A0F	UniTrust Event Certificate Root CA R1
UniTrust Global Root CA R1	Root Key	sha384RSA	4096 bits	3c a0 61 b0 ef da c6 e8 bb 2d e1 56 a2 eb bb b6 3d 23 23 81	81B35EFC42C7794 7209D76B51B5E7B 122CE78348AE8C4 525DC8D4B30289 E5385	UniTrust Global Root CA R1
UniTrust Global Root CA R2	Root Key	sha384ECDSA	384 bits	e4 53 66 b7 b7 a4 e9 d7 cc c1 21 e0 4a cf cc ac 01 bc 72 bc	78919B35D1C61559 5A51328A5C54608 3B4D5320724A258 695B991F2F61C4D CC7	UniTrust Global Root CA R2
UniTrust Global Root CA R3	Root Key	SM2	256 bits	3b 15 e6 2b 1c 9f 50 15 b6 4e a1 6d 16 3a 55 8a f4 90 5f b5	6A19BCC7FAD2A56 64F779BF143A72A 2B079AC476E56FA CBA48C352635CB4 718F	UniTrust Global Root CA R3