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, 2024 to March 31, 2025, for its CAs enumerated in Attachment A, SHECA has:

- disclosed its SSL certificate lifecycle management business practices in its:
  - UniTrust Certification Practice Statement v3.7.9;
  - UniTrust Certification Practice Statement v3.7.8;
  - UniTrust Certification Practice Statement v3.7.7;
  - UniTrust Certificate Policy v1.5.7;
  - UniTrust Certificate Policy v1.5.6; and
  - UniTrust Certificate Policy v1.5.5,

  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,

in accordance with the WebTrust Principles and Criteria for Certification Authorities - SSL Baseline v2.8.

Management's Responsibilities

SHECA's management is responsible for the management's assertion, including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities - SSL Baseline v2.8.

Our Independence and Quality Management

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

Our firm applies International Standard on Quality Management 1, which requires the firm to design, implement and operate a system of quality management including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Practitioner's Responsibilities

It is our responsibility to express an opinion on the management's assertion based on our work performed.

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

A reasonable assurance engagement involves performing procedures to obtain sufficient appropriate evidence whether the management's assertion of SHECA is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities - SSL Baseline v2.8. The extent of procedures selected depends on the practitioner's judgment and our assessment of the engagement risk. Within the scope of our work we performed amongst others the following procedures: (1) obtaining an understanding of SHECA's SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of SSL certificates; (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 April 1, 2024 to March 31, 2025, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities - SSL Baseline v2.8.

Emphasis of Matter

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 v2.8, nor the suitability of any of SHECA's services for any customer's intended purpose. Our opinion is not modified in respect of this matter.

Other Matters

The UniTrust Global Root CA R1 (Attachment A #53), UniTrust Global Root CA R2 (Attachment A #57), UniTrust Global TLS ECC Root CA R2 (Attachment A #61), and UniTrust Global TLS RSA Root CA R1 (Attachment A #65) CAs did not issue certificates during the period April 1, 2024 to March 31, 2025 and were maintained online to provide revocation status information only.

SHECA's management has disclosed 4 incidents (see Attachment B) during the period from April 1, 2024 to March 31, 2025. 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.

Our opinion is not modified in respect of these matters.

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 v2.8 designed for this purpose. As a result, the management's assertion of SHECA may not be suitable for another purpose. This report is intended solely for the management of SHECA in connection with obtaining and displaying the WebTrust Seal on its website after submitting the report to the related authority in

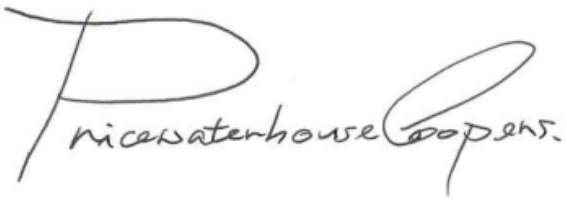
[1] *The maintenance and integrity of the SHECA website is the responsibility of the management of SHECA; the work carried out by the assurance provider does not involve consideration of these matters and, accordingly, the assurance provider accepts no responsibility for any differences between the accompanying 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.*

connection with the WebTrust Principles and Criteria for Certification Authorities - SSL Baseline v2.8.

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

Use of the WebTrust seal

SHECA's use of the WebTrust for Certification Authorities - SSL Baseline 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, 9 May 2025

Attachment A

The list of keys and certificates in scope for the period from April 1, 2024 to March 31, 2025 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 Domain Validation Server CA G3	Signing Key	sha256RSA	2048 bits	CN = SHECA RSA Domain Validation Server CA G3 O = UniTrust C = CN	057A4D756FFD0A83B1671675773E14C5F53C548E	0A552A65F22FF820E7EC3D43BBF88B02ABC34BD247E0C3505891B6342F16A5F2	UCA Global G2 Root
3	SHECA RSA Organization Validation Server CA G3	Signing Key	sha256RSA	2048 bits	CN = SHECA RSA Organization Validation Server CA G3 O = UniTrust C = CN	316068091E32F9F6CCC06215AA7B91AF4C119D40	26FD4C4367E463D39C71796AE4010E53380DC93BC132FB019D6718A6873E81F4	UCA Global G2 Root
4	SHECA DV Server CA G5	Signing Key	sha256RSA	2048 bits	CN = SHECA DV Server CA G5 O = UniTrust C = CN	D8E7061B645FAB3008887A2453AAE11C8304BF6D	778C516DAEC700EE58B3581E411E5C0DD478663A5163A29895341507D6E964DD	UCA Global G2 Root
5	SHECA OV Server CA G5	Signing Key	sha256RSA	2048 bits	CN = SHECA OV Server CA G5 O = UniTrust C = CN	0379A38D525FD4E988921F4358542502F4878B7E	8AB3A0ACF289E6EF754BE449236843D67F45C191BDDD66484B85E6E60556A9AF	UCA Global G2 Root
6	SHECA EV Server CA G2	Signing Key	sha256RSA	2048 bits	CN = SHECA EV Server CA G2 O = UniTrust C = CN	86B148C0420A9C6F81FC4FDCD10F184BAAB5A6EA	4216527163AD2CAA825D3BF48F61A7661D0ABC89B58AB76B23A1E10999F0769F	UCA Global G2 Root
7	TrustAsia RSA DV TLS CA - S1	Signing Key	sha256RSA	2048 bits	CN = TrustAsia RSA DV TLS CA - S1 O = TrustAsia Technologies, Inc. C = CN	9432E0D48ACD1D93E75C5372960C5EF1F3F67972	074ADD7F1E73EB110EC8E2B78A92C51CF5A451135B6F7DEFC019EE9D74BFA4D6	UCA Global G2 Root
8	TrustAsia RSA OV TLS CA - S1	Signing Key	sha256RSA	2048 bits	CN = TrustAsia RSA OV TLS CA - S1 O = TrustAsia Technologies, Inc. C = CN	F575D48E293E17A8A9C49EDCE6DB0A344D132AEB	D16BA9ACB74FEE4AA8087EE482E86E7F6F5F55FAC5025639730753FE1E705E3C	UCA Global G2 Root

#	Key Name	Key Type	Signature Algorithm	Key Size	Subject DN	Subject Key Identifier	Certificates Thumbprint (SHA256)	Certificate Signed by
9	SHECA Global G3 SSL	Signing Key	sha256RSA	2048 bits	CN = SHECA Global G3 SSL O = UniTrust S = Shanghai C = CN	9820F0F1D942A6DE833F991019003D6868D20181	AEFFE4335EE56422E927F45E95AE142B9EB35979A7400569AE9BDEA6CAABC1DC	UCA Global G2 Root
10	Xinnet DV SSL	Signing Key	sha256RSA	2048 bits	CN = Xinnet DV SSL O = 北京新网数码信息技术有限公司 C = CN	9D3AA5B8E2212783643FF578DC22B04E6BCB36D4	9C53902F9501F6D89766999DBE2AD1A1436420B652535CDC2DC51CCFE2FFEE68	UCA Global G2 Root
11	Xinnet OV SSL	Signing Key	sha256RSA	2048 bits	CN = Xinnet OV SSL O = 北京新网数码信息技术有限公司 C = CN	4B78C0324A2442784E9F83F0D0FE336C7E0D934F	3C07D7EFC8D458F668C10D4F06F90503CCD25D59E2B3F1D58B32884D9E4E3809	UCA Global G2 Root
12	JoySSL DV Secure Server CA G1	Signing Key	sha384RSA	3072 bits	CN = JoySSL DV Secure Server CA G1 O = JoySSL Limited C = CN	2A56E8EF40E0A9999D6DD8129FB79B056B882DED	AA9CD0737407E9E9D9D86B145A2CFD7CD385C28BCF5996AA8D9A6DA5FC76F3A2	UCA Global G2 Root
13	JoySSL OV Secure Server CA G1	Signing Key	sha384RSA	3072 bits	CN = JoySSL OV Secure Server CA G1 O = JoySSL Limited C = CN	6BF2449C86D0C6DED85107661B2748792342CB95	0DD33FA366CA02808D29A5C1C456496AB5015C3604EB21C101406AF2533D998A	UCA Global G2 Root
14	KeepTrust DV TLS RSA CA G2	Signing Key	sha384RSA	3072 bits	CN = KeepTrust DV TLS RSA CA G2 O = Shanghai Huandu Info Tech Co. Ltd. C = CN	088B0DF30B0966297021D02C377300F5A7F4E7E9	352582CCC85B3944E3CD2505D9318F22ABEA418BFF29A0FE4D2C0DF280F200E3	UCA Global G2 Root
15	KeepTrust OV TLS RSA CA G2	Signing Key	sha384RSA	3072 bits	CN = KeepTrust OV TLS RSA CA G2 O = Shanghai Huandu Info Tech Co. Ltd. C = CN	F68D3850B96EA8BEFC50CA91247F1ABC9EA39D4D	CD50559A6DC5C704237EABF9A070B79F0CDFC1A79C3A6AC8C5E71E295A065D0A	UCA Global G2 Root

#	Key Name	Key Type	Signature Algorithm	Key Size	Subject DN	Subject Key Identifier	Certificates Thumbprint (SHA256)	Certificate Signed by
16	ZoTrus RSA DV SSL CA G1	Signing Key	sha384RSA	3072 bits	CN = ZoTrus RSA DV SSL CA G1 O = ZoTrus Technology Limited C = CN	EC1EBCB71E092769EFA715E89AA1677C33AA0F5A	E7EF1AD946214B32AF03CC287930D0464ED2C086D7A1447C6E27FC9217D4E16B	UCA Global G2 Root
17	ZoTrus RSA OV SSL CA G1	Signing Key	sha384RSA	3072 bits	CN = ZoTrus RSA OV SSL CA G1 O = ZoTrus Technology Limited C = CN	A0FA64A37EB83C7C194C51B7FE6A2BE8A39F78A4	3EC123D71DB27AE1DC8F877286C222F4167A2AE4FD7BCF370789EF4A9521B8	UCA Global G2 Root
18	JoySSL DV Secure Server CA	Signing Key	sha384RSA	3072 bits	CN = JoySSL DV Secure Server CA O = JoySSL Limited C = CN	807B3118B837D850FD1C4AD9879A5E426D00A1A4	AA9CD0737407E9E9D9D86B145A2CFD7CD385C28BCF5996AA8D9A6DA5FC76F3A2	UCA Global G2 Root
19	JoySSL OV Secure Server CA	Signing Key	sha384RSA	3072 bits	CN = JoySSL OV Secure Server CA O = JoySSL Limited C = CN	21507E5079E680B202C0FBC1AFAD8026DC52B8DD	0DD33FA366CA02808D29A5C1C456496AB5015C3604EB21C101406AF2533D998A	UCA Global G2 Root
20	KeepTrust DV TLS RSA CA G1	Signing Key	sha384RSA	3072 bits	CN = KeepTrust DV TLS RSA CA G1 O = Shanghai Huandu Info Tech Co. Ltd. C = CN	5063446A28FAC2B3D5122D01A63D9B85845026CC	A879CB01A2661C255B9C2B9BE0B20BA74EEA9546E21A82C570E177CF5BF4AEDA	UCA Global G2 Root
21	KeepTrust OV TLS RSA CA G1	Signing Key	sha384RSA	3072 bits	CN = KeepTrust OV TLS RSA CA G1 O = Shanghai Huandu Info Tech Co. Ltd. C = CN	04FA1B9DBC05CD575CC6518D5CDFE62CD151B0C8	FFD0D9EEEAAFBB4C44F71392F20A52E0F6589685493313964072 2DECFC2D4658	UCA Global G2 Root
22	ZoTrus RSA DV SSL CA	Signing Key	sha384RSA	3072 bits	CN = ZoTrus RSA DV SSL CA O = ZoTrus Technology Limited C = CN	7FEF9B0B9EB3F717A576BBC7580209DE731544B7	69C25861236502F0C223443FD851A2FB6ACB745BB814AD72BB2E50867C52C3BB	UCA Global G2 Root

#	Key Name	Key Type	Signature Algorithm	Key Size	Subject DN	Subject Key Identifier	Certificates Thumbprint (SHA256)	Certificate Signed by
23	ZoTrus RSA OV SSL CA	Signing Key	sha384RSA	3072 bits	CN = ZoTrus RSA OV SSL CA O = ZoTrus Technology Limited C = CN	E92D57AB2A4455799E257937123588FCDF187AC3	219C59CCD06D0210ADCF6E8125700D1578F69A0670A07FD9DDE99E4AC82524CD	UCA Global G2 Root
24	CT2 DV TLS RSA CA G1	Signing Key	sha384RSA	3072 bits	CN = CT2 DV TLS RSA CA G1 O = Tianyi Security Technology Co., Ltd. C = CN	8955C1DB0608F7A83C51CA3BF98F017B90098A73	4B316EDFC0780286571E430C0A94231B192B45666AF5DEBEE454FE08E4496383	UCA Global G2 Root
25	CT2 OV TLS RSA CA G1	Signing Key	sha384RSA	3072 bits	CN = CT2 OV TLS RSA CA G1 O = Tianyi Security Technology Co., Ltd. C = CN	27937BF574A8AF23A7F29E2B03CFACC7182B2EFA	A263B7CEFD1490D04FD0EC31D9695BAEE480EE861D12124C2BF8EBD8A893652F	UCA Global G2 Root
26	SHECA FREE DV TLS RSA CA G1	Signing Key	sha384RSA	3072 bits	CN = SHECA FREE DV TLS RSA CA G1 O = UniTrust C = CN	F18082839D6BB5C20A6A43C2D584A9F6F3EF2DC9	DFD9FB07A42E81216D6497FBC47BE53D829BBFD6A9188B02D5C8CDE29E01CF5C	UCA Global G2 Root
27	SHECA FREE DV TLS ECC CA G2	Signing Key	sha384RSA	384 bits	CN = SHECA FREE DV TLS ECC CA G2 O = UniTrust C = CN	84BCFE29594A85C0849FF0F21230812BE73F9BBC	81DB88F4CDE7345B0EC140E4A193720163DF9B787FABA0AF5A7EDACE6DC315A6	UCA Global G2 Root
28	SHECA DV TLS ECC CA G6	Signing Key	sha384RSA	384 bits	CN = SHECA DV TLS ECC CA G6 O = UniTrust C = CN	7E44A7C621F5F30E25293C07F288ECC82F7BD482	1F0570E418F9C89E094CB26EDA71B92BED81ACBB446B2300D398DDB739AB7A6C	UCA Global G2 Root
29	SHECA OV TLS ECC CA G6	Signing Key	sha384RSA	384 bits	CN = SHECA OV TLS ECC CA G6 O = UniTrust C = CN	2569CCEFDB564A83BAC15284500F13D86104FEE0	C4DA2C937523D42054FBB4AF694BB90FC7743C910EE048726241BD84C38509D9	UCA Global G2 Root
30	DNSPod DV TLS RSA CA G1	Signing Key	sha384RSA	3072 bits	CN = DNSPod DV TLS RSA CA G1 O = DNSPod, Inc. C = CN	4CF1C77BBB5F991923F8616FD712F9749C5AE55C	A07A7DEFCD1ED23F36D22AC33421F1D973583B12C96CA2496DE724C4494C0CD2	UCA Global G2 Root

#	Key Name	Key Type	Signature Algorithm	Key Size	Subject DN	Subject Key Identifier	Certificates Thumbprint (SHA256)	Certificate Signed by
31	DNSPod DV TLS ECC CA G1	Signing Key	sha384RSA	384 bits	CN = DNSPod DV TLS ECC CA G1 O = DNSPod, Inc. C = CN	B9A7EB6345A DB88940892F 8B69930658D A9733CF	AACCD77057271FF5F 605DF8CC5A44397E7 1CCE796EA79B8F1E8 658FC9CD52464	UCA Global G2 Root
32	DNSPod OV TLS RSA CA G1	Signing Key	sha384RSA	3072 bits	CN = DNSPod OV TLS RSA CA G1 O = DNSPod, Inc. C = CN	38C22FB4856 AB84A51911F E53A7FE2BE1 103338F	F36592E33FD869E91 7E33BADE683A4EC2 0809D5C8B493A1427 BA6DC066CB5AE3	UCA Global G2 Root
33	DNSPod OV TLS ECC CA G1	Signing Key	sha384RSA	384 bits	CN = DNSPod OV TLS ECC CA G1 O = DNSPod, Inc. C = CN	586EA657334 43DCE3CED5 DEBF47E000 F0E81B28D	8C4BFF9AE3F079E50 208F84E4DA658AB4 41109686861FFCEE50 D4A8662C2EEA1	UCA Global G2 Root
34	Keymatic Secure Domain RSA CA G1	Signing Key	sha384RSA	3072 bits	CN = Keymatic Secure Domain RSA CA G1 O = PKI(Chongqing) Limited C = CN	8ED096D6E8 A4D935F386E BDA0B592E4 0521B0CBB	F3C9431A163BECE79 562093F0734DF6ED0 5618551CFEE0ABA94 9A77E959D8AAE	UCA Global G2 Root
35	Keymatic Secure Domain ECC CA G1	Signing Key	sha384RSA	384 bits	CN = Keymatic Secure Domain ECC CA G1 O = PKI(Chongqing) Limited C = CN	C1286B590B1 98916D776E6 661E57D4460 812EDDF	B07D2ACA4F29E2449 B5ADB7CCB31C64C43 854044A2DAA2AC83 8788026C684C0C	UCA Global G2 Root
36	Keymatic Secure Business RSA CA G1	Signing Key	sha384RSA	3072 bits	CN = Keymatic Secure Business RSA CA G1 O = PKI(Chongqing) Limited C = CN	5693F449C7E 448C3C3D2BE 86397E333681 63A377	5523644185E21EF943 A505A1C438167DA1F E7B14BEF2D243E53D E8C2B4263EB7	UCA Global G2 Root
37	Keymatic Secure Business ECC CA G1	Signing Key	sha384RSA	384 bits	CN = Keymatic Secure Business ECC CA G1 O = PKI(Chongqing) Limited C = CN	23368DE013A 9BB36D76A66 E1128EDA5F4 A3620D5	75C4AF6628E7D01DD 369593EFD727E3560 ED9DDD67B0432565 5821BD23281A2B	UCA Global G2 Root
38	sslTrus RSA DV TLS CA G2	Signing Key	sha384RSA	3072 bits	CN = sslTrus RSA DV TLS CA G2 O = sslTrus C = CN	DEE386BAC5 2E630164E0C 142943C32029 67C6891	B3A5BED750BCE5A0 8C75E0012B0A6A679 54952BC8D12520514C C15CBB0B17039	UCA Global G2 Root

#	Key Name	Key Type	Signature Algorithm	Key Size	Subject DN	Subject Key Identifier	Certificates Thumbprint (SHA256)	Certificate Signed by
39	sslTrus ECC DV TLS CA G2	Signing Key	sha384RSA	384 bits	CN = sslTrus ECC DV TLS CA G2 O = sslTrus C = CN	624679EBA47 FFA4CD98D6 FFFDE6D6F7 FE49E86E9	32CAA961415106CF47 1CEA5B15C66464A90 7C99861A297C359D17 4624BADB92F	UCA Global G2 Root
40	sslTrus RSA OV TLS CA G2	Signing Key	sha384RSA	3072 bits	CN = sslTrus RSA OV TLS CA G2 O = sslTrus C = CN	0EDFB68948 064E10818E3 C8108C824BB 8B308F62	F0E647B5A2869A348 7507A90549AF03989 6DB8B0F0E7CF92EF 3AB567F3EC5E5C	UCA Global G2 Root
41	sslTrus ECC OV TLS CA G2	Signing Key	sha384RSA	384 bits	CN = sslTrus ECC OV TLS CA G2 O = sslTrus C = CN	BEE114C1BEF 84DA5E3D4E 41FCA0D1F81 A90C0FE0	06B7E611243D2901B9 64FF6D0C53A2DB52 BA2E1D41E17D74950 E16605D9A2C90	UCA Global G2 Root
42	HTTPS Automati on Research RSA DV SSL CA G1	Signing Key	sha384RSA	3072 bits	CN = HTTPS Automation Research RSA DV SSL CA G1 O = Shenzhen Yamu Security Technology Co., Ltd. C = CN	0FB6A84D71E 5B1B38F9E72 D6BBC06A147 FE4D03B	1E426FF0F51EB4C28 5788B4418D2DAB210 97230CED81119BA178 A20AB1AABF67	UCA Global G2 Root
43	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E 430FFA50C08 5F8C15672174 01DFDF	C1AFC65B1E813B0E6 146E6AA5341681272A BE9A38D59F7BD1B27 B729834A0D9C	Certum Trusted Network CA
44	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E 430FFA50C08 5F8C15672174 01DFDF	3DD69C5BE170F943F 804D1D31FE8F916C0 C0226CDDD7AEA9AA 9A0CDFD3474361	Certum Trusted Network CA
45	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E 430FFA50C08 5F8C15672174 01DFDF	BB61408AED9F530B2 EC0545E53BA2C8EB EAA57D9976447DB16 63CED4600CD6B7	Certum Trusted Network CA
46	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E 430FFA50C08 5F8C15672174 01DFDF	BFA95C5DF164B659F A32F6D10564D7170D DE661A853A782E6AB 63639433BCB41	Certum Trusted Network CA
47	UCA Extended Validatio n Root	Root Key	sha256RSA	4096 bits	CN = UCA Extended Validation Root O = UniTrust C = CN	D9743AE4303 D0DF712DC7 E5A059F1E34 9AF7E114	D43AF9B35473755C9 684FC06D7D8CB70E E5C28E773FB294EB4 1EE71722924D24	UCA Extended Validation Root
48	SHECA RSA Extended Validatio n Server CA	Signing Key	sha256RSA	2048 bits	CN = SHECA RSA Extended Validation Server CA O = UniTrust C = CN	3B4B252A773 72AFCB97FED A8BDAF2299 FC5DC5F4	4FD6FA527157EEA46 3689D7A4C2B934EF2 22279725413893D984 7242C85CA9DF	UCA Extended Validation Root

#	Key Name	Key Type	Signature Algorithm	Key Size	Subject DN	Subject Key Identifier	Certificates Thumbprint (SHA256)	Certificate Signed by
49	SHECA EV Server CA G3	Signing Key	sha256RSA	2048 bits	CN = SHECA EV Server CA G3 O = UniTrust C = CN	54E972FB78669FE5CBF33B8F98465553739C0B84	7EF3F89456CE636557B20C5DFB37F98C253A0B660D2E9E5E7845CAF9C038C7C1	UCA Extended Validation Root
50	SHECA OV Server CA G6	Signing Key	sha256RSA	2048 bits	CN = SHECA OV Server CA G6 O = UniTrust C = CN	FB7DCE4905B420BCFFBF0D8471ADAE0135F961A0	264DF1458FB5EF1FC9DF9F1345E84A6CC1A471CF475AE7598FF52B86713519FB	UCA Extended Validation Root
51	SHECA OV Server CA G7	Signing Key	sha256RSA	2048 bits	CN = SHECA OV Server CA G7 O = UniTrust C = CN	A0F344BA17512C7776AB4442C5534B16AB5F0DAA	F6F8BCD413C9733166E85843B468DD36E727152D9A37B15129C0E7648ECEE639	UCA Extended Validation Root
52	SHECA Extended Validation SSL CA	Signing Key	sha256RSA	2048 bits	CN = SHECA Extended Validation SSL CA O = UniTrust C = CN	4D140DEA6B559C0CA6E1BB7BE86A966D175E7CB5	25BFDB1C5FE2CCE051EC6DFBF2BB24E78C92F969B1BB37867DAEDF93D1A7AE7E	UCA Extended Validation Root
53	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
54	SHECA DV Server CA 1A	Signing Key	sha384RSA	4096 bits	CN = SHECA DV Server CA 1A O = UniTrust C = CN	653740E0BBF43905206A8C9CA0ACB3BBD6968CA0	D3D4A040BB41A695A96E3AAD93814CF7EF219D5819206E947B44DCC5B8E5E272	UniTrust Global Root CA R1
55	SHECA OV Server CA 1A	Signing Key	sha384RSA	4096 bits	CN = SHECA OV Server CA 1A O = UniTrust C = CN	8CD02E82008EE2DEFF71F61A105C74A826E858D1	9A3DB0F0FB0FF4F974A4E0C510A7C13D350485B1E6CDF5A899BB24D0F499E9BD	UniTrust Global Root CA R1
56	SHECA EV Server CA 1A	Signing Key	sha384RSA	4096 bits	CN = SHECA EV Server CA 1A O = UniTrust C = CN	73E36DF62D862F57DF69A53687231C85E0170216	2F1CA1A5C0D7AE58C7ADFC69D4C57EE815F39C0F3D1F982E3AC76D25AB723995	UniTrust Global Root CA R1
57	UniTrust Global Root CA R2	Root Key	sha384ECDSA	384 bits	CN = UniTrust Global Root CA R2 O = UniTrust C = CN	E45366B7B7A4E9D7CCC121E04ACFCCAC01BC72BC	78919B35D1C615595A51328A5C546083B4D5320724A258695B991F2F61C4DCC7	UniTrust Global Root CA R2
58	SHECA DV Server CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA DV Server CA 2A O = UniTrust C = CN	A1221170BEC8665F6ECB104C4EDB38EA9C1F914D	69201DC24E4127FFA5B41A0DDF0A1A005C00F334B003F1008924CBF998E1827C	UniTrust Global Root CA R2

#	Key Name	Key Type	Signature Algorithm	Key Size	Subject DN	Subject Key Identifier	Certificates Thumbprint (SHA256)	Certificate Signed by
59	SHECA OV Server CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA OV Server CA 2A O = UniTrust C = CN	98CDEC338767F39422373810B735BA7C683A8259	8E2CA2825C2039804A7A1CC54B002EA1DB30AC489698F039527BF1602132F611	UniTrust Global Root CA R2
60	SHECA EV Server CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA EV Server CA 2A O = UniTrust C = CN	44661C71EF69B7930AB5B771D83B114CFA843D77	93E49170D20F54DA701118A5ABDCDDA4FFCF334CDB2D8D80599AB62848C85F80	UniTrust Global Root CA R2
61	UniTrust Global TLS ECC Root CA R2	Root Key	sha384ECDSA	384 bits	CN = UniTrust Global TLS ECC Root CA R2 O = UniTrust C = CN	7935AD798A95305C3E05A675161A97000F6FCC90	6C689FC6B014A1FB0CDEB5A3996171C15E7286106028532E0210CEA8D9CD4E97	UniTrust Global TLS ECC Root CA R2
62	SHECA DV TLS ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA DV TLS ECC CA 2A O = UniTrust C = CN	CB65E62F50175F2C172B433F3A043CD213569A66	D690D8722EA89CD7617901449520653339386AC4939F7EC5C1B195D9C3C95FA4	UniTrust Global TLS ECC Root CA R2
63	SHECA EV TLS ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA EV TLS ECC CA 2A O = UniTrust C = CN	B353900B5E40A4952EA85A27F413ABBAD631F233	05E4C4B1F258030690E6793C9C13C6F6AE234F68E5C41236FDC919B7F589032F	UniTrust Global TLS ECC Root CA R2
64	SHECA OV TLS ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA OV TLS ECC CA 2A O = UniTrust C = CN	A065578C43B2546C4E18DF86AED56725A9B7659C	08BA64405A3406C97BDCBD0E44224E6DD341F3EC93F1368457DFA7CAC88BE150	UniTrust Global TLS ECC Root CA R2
65	UniTrust Global TLS RSA Root CA R1	Root Key	sha384RSA	4096 bits	CN = UniTrust Global TLS RSA Root CA R1 O = UniTrust C = CN	F2ADBFAB6708F09672E633D65175A24759C900C4	4BABE0E9328D5DAE17936F3DDAA2442BFBDD0873F92FB8D1FBBD3D9894649AD9	UniTrust Global TLS RSA Root CA R1
66	SHECA DV TLS RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA DV TLS RSA CA 1A O = UniTrust C = CN	C5E3A87F7EEDBC3E7108B34EF490EF2F2F1367D1	FFABEA74895DC0C78C224597472CF6937E0D740EF49DC2256C8E75A2A2A15EDE	UniTrust Global TLS RSA Root CA R1
67	SHECA EV TLS RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA EV TLS RSA CA 1A O = UniTrust C = CN	60651A135EAB2B98A5A1041B3057A1D02FC612E5	B2525A5966CA68CA7F504F0A21FD73847D174F89B48852A3E970588E1EAFC774	UniTrust Global TLS RSA Root CA R1
68	SHECA OV TLS RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA OV TLS RSA CA 1A O = UniTrust C = CN	F463091C1E2788B75DBBE91644B1744A34F34B46	7F8EF707C2D9A4B7D4ED5FDDC8AF4A64D99BF297D03F8F01C4375DE74B1C7DE1	UniTrust Global TLS RSA Root CA R1

Attachment B - Publicly disclosed incidents

The list of incidents disclosed publicly during the period from April 1, 2024 to March 31, 2025 is as follow:

Bugzilla ID	Disclosure	Publicly Disclosed Link
1902592	SHECA: EV certificate subject RDN order is incorrect	Bugzilla Ticket Link
1902947	SHECA: The certificate's cpsURI is empty	Bugzilla Ticket Link
1914365	SHECA: CRLReason code usage error	Bugzilla Ticket Link
1946921	SHECA: DV SSL certificate format is abnormal	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 2024 年 4 月 1 日至 2025 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 v3.7.9；
  - UniTrust证书认证业务规则v3.7.8；
  - UniTrust证书认证业务规则 v3.7.7；
  - UniTrust证书策略 v1.5.7；
  - UniTrust证书策略 v1.5.6；以及
  - UniTrust证书策略 v1.5.5，

  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，

以符合 WebTrust 电子认证 SSL 基准规范审计标准 v2.8.

管理层的责任

SHECA的管理层负责确保管理层认定，包括其陈述的客观性以及认定中描述的SHECA所提供的服务能够符合WebTrust电子认证 - SSL基准规范审计标准v2.8的规定。

我们的独立性和质量管理

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

本事务所遵循国际质量管理准则第 1 号，该准则要求事务所设计、实施并执行质量管理体系，包括与遵守职业道德要求、专业标准和适用的法律和法规要求的政策或程序。

注册会计师的责任

我们的责任是在执行鉴证工作的基础上对管理层认定发表意见。

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

合理保证的鉴证业务涉及实施鉴证程序，以获取有关管理层认定是否在所有重大方面符合 WebTrust 电子认证 - SSL 基准规范审计标准 v2.8 的充分、适当的证据。选择的鉴证程序取决于注册会计师的判断及我们对项目风险的评估。在我们的工作范围内，我们实施了包括（1）了解 SHECA SSL 证书生命周期管理，包括 SSL 证书发放、更新和吊销的相关控制，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。

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 2024 年 4 月 1 日至 2025 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 基准规范审计标准 v2.8。

强调事项

我们提请使用者关注，本报告并不包括任何在 WebTrust 电子认证 - SSL 基准规范审计标准 v2.8 以外的质量标准声明，或对任何客户对 SHECA 服务的合适性声明。本段内容不影响已发表的鉴证意见。

其他事项

UniTrust Global Root CA R1（附录A#53），UniTrust Global Root CA R2（附录A#57），UniTrust Global TLS ECC Root CA R2（附录 A#61）和 UniTrust Global TLS RSA Root CA R1（附录 A#65）在 2024 年 4 月 1 日至 2025 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 2024年4月1日至2025年3月31日期间，SHECA 管理层披露了 4 起事件（见附录 B）。SHECA 所采取的补救措施和这些事件的根本原因已在 Bugzilla 网站的在线论坛以及组成 CA/Browser 论坛的各个互联网浏览器的在线论坛上公开发布。本段内容不影响已发表的鉴证意见。

目的及使用和分发限制

管理层认定为在 SHECA 网站[1]上获取并展示 WebTrust Seal 编制，并采用为该目的而设计的 WebTrust 电子认证 - SSL 基准规范审计标准 v2.8，因此后附 SHECA 管理层认定可能不适用于其他目的。本报告仅向 SHECA 管理层出具，用作向 WebTrust 电子认证 - SSL 基准规范审计标准 v2.8 相关机构提交报告后，在 SHECA 网站上获取并展示 WebTrust Seal，不应向任何其它方分发或为其他目的使用。我们不会就本报告的内容向任何其他人士负上或承担任何责任。

WebTrust seal 的使用

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

罗兵咸永道会计师事务所
注册会计师

香港，2025 年 5 月 9 日

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

pwc

羅兵咸永道

附录 A

下表列示了 2024 年 4 月 1 日至 2025 年 3 月 31 日期间本报告范围内的密钥和证书：

#	密钥名称	密钥种类	密钥算法	密钥长度	主体识别名	密钥 ID	证书指纹（SHA256）	证书签发者
1	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	9BEA11C976FE014764C1BE56A6F914B5A5600317ABD9988393382E5161AA0493C	UCA Global G2 Root
2	SHECA RSA Domain Validation Server CA G3	Signing Key	sha256RSA	2048 bits	CN = SHECA RSA Domain Validation Server CA G3 O = UniTrust C = CN	057A4D756FFD0A83B1671675773E14C5F53C548E	0A552A65F22FF820E7EC3D43BBF88B02ABC34BD247E0C3505891B6342F16A5F2	UCA Global G2 Root
3	SHECA RSA Organization Validation Server CA G3	Signing Key	sha256RSA	2048 bits	CN = SHECA RSA Organization Validation Server CA G3 O = UniTrust C = CN	316068091E32F9F6CCC06215AA7B91AF4C119D40	26FD4C4367E463D39C71796AE4010E53380DC93BC132FB019D6718A6873E81F4	UCA Global G2 Root
4	SHECA DV Server CA G5	Signing Key	sha256RSA	2048 bits	CN = SHECA DV Server CA G5 O = UniTrust C = CN	D8E7061B645FAB3008887A2453AAE11C8304BF6D	778C516DAEC700EE58B3581E411E5C0DD478663A5163A29895341507D6E964DD	UCA Global G2 Root
5	SHECA OV Server CA G5	Signing Key	sha256RSA	2048 bits	CN = SHECA OV Server CA G5 O = UniTrust C = CN	0379A38D525FD4E988921F4358542502F4878B7E	8AB3A0ACF289E6EF754BE449236843D67F45C191BDDD66484B85E6E60556A9AF	UCA Global G2 Root
6	SHECA EV Server CA G2	Signing Key	sha256RSA	2048 bits	CN = SHECA EV Server CA G2 O = UniTrust C = CN	86B148C0420A9C6F81FC4FDCD10F184BAAB5A6EA	4216527163AD2CAA825D3BF48F61A7661D0ABC89B58AB76B23A1E10999F0769F	UCA Global G2 Root

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
7	TrustAsia RSA DV TLS CA - S1	Signing Key	sha256RSA	2048 bits	CN = TrustAsia RSA DV TLS CA - S1 O = TrustAsia Technologies, Inc. C = CN	9432E0D48ACD1D93E75C5372960C5EF1F3F67972	074ADD7F1E73EB110EC8E2B78A92C51CF5A451135B6F7DEFC019EE9D74BFA4D6	UCA Global G2 Root
8	TrustAsia RSA OV TLS CA - S1	Signing Key	sha256RSA	2048 bits	CN = TrustAsia RSA OV TLS CA - S1 O = TrustAsia Technologies, Inc. C = CN	F575D48E293E17A8A9C49EDCE6DB0A344D132AEB	D16BA9ACB74FEE4AA8087EE482E86E7F6F5F55FAC5025639730753FE1E705E3C	UCA Global G2 Root
9	SHECA Global G3 SSL	Signing Key	sha256RSA	2048 bits	CN = SHECA Global G3 SSL O = UniTrust S = Shanghai C = CN	9820F0F1D942A6DE833F991019003D6868D20181	AEFFE4335EE56422E927F45E95AE142B9EB35979A7400569AE9BDEA6CAABC1DC	UCA Global G2 Root
10	Xinnet DV SSL	Signing Key	sha256RSA	2048 bits	CN = Xinnet DV SSL O = 北京新网数码信息技术有限公司 C = CN	9D3AA5B8E2212783643FF578DC22B04E6BCB36D4	9C53902F9501F6D89766999DBE2AD1A1436420B652535CDC2DC51CCFE2FFEE68	UCA Global G2 Root
11	Xinnet OV SSL	Signing Key	sha256RSA	2048 bits	CN = Xinnet OV SSL O = 北京新网数码信息技术有限公司 C = CN	4B78C0324A2442784E9F83F0D0FE336C7E0D934F	3C07D7EFC8D458F668C10D4F06F90503CCD25D59E2B3F1D58B32884D9E4E3809	UCA Global G2 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
12	JoySSL DV Secure Server CA G1	Signing Key	sha384RSA	3072 bits	CN = JoySSL DV Secure Server CA G1 O = JoySSL Limited C = CN	2A56E8EF40E0A9999D6DD8129FB79B056B882DED	AA9CD0737407E9E9D9D86B145A2CFD7CD385C28BCF5996AA8D9A6DA5FC76F3A2	UCA Global G2 Root
13	JoySSL OV Secure Server CA G1	Signing Key	sha384RSA	3072 bits	CN = JoySSL OV Secure Server CA G1 O = JoySSL Limited C = CN	6BF2449C86D0C6DED85107661B2748792342CB95	0DD33FA366CA02808D29A5C1C456496AB5015C3604EB21C101406AF2533D998A	UCA Global G2 Root
14	KeepTrust DV TLS RSA CA G2	Signing Key	sha384RSA	3072 bits	CN = KeepTrust DV TLS RSA CA G2 O = Shanghai Huandu Info Tech Co. Ltd. C = CN	088B0DF30B0966297021D02C377300F5A7F4E7E9	352582CCC85B3944E3CD2505D9318F22ABEA418BFF29A0FE4D2C0DF280F200E3	UCA Global G2 Root
15	KeepTrust OV TLS RSA CA G2	Signing Key	sha384RSA	3072 bits	CN = KeepTrust OV TLS RSA CA G2 O = Shanghai Huandu Info Tech Co. Ltd. C = CN	F68D3850B96EA8BEFC50CA91247F1ABC9EA39D4D	CD50559A6DC5C704237EABF9A070B79F0CDFC1A79C3A6AC8C5E71E295A065D0A	UCA Global G2 Root
16	ZoTrus RSA DV SSL CA G1	Signing Key	sha384RSA	3072 bits	CN = ZoTrus RSA DV SSL CA G1 O = ZoTrus Technology Limited C = CN	EC1EBCB71E092769EFA715E89AA1677C33AA0F5A	E7EF1AD946214B32AF03CC287930D0464ED2C086D7A1447C6E27FC9217D4E16B	UCA Global G2 Root
17	ZoTrus RSA OV SSL CA G1	Signing Key	sha384RSA	3072 bits	CN = ZoTrus RSA OV SSL CA G1 O = ZoTrus Technology Limited C = CN	A0FA64A37EB83C7C194C51B7FE6A2BE8A39F78A4	3EC123D71DB27AE1DC8F877286C222F4167A2AE4FD7BCF370789EF4A9521B8	UCA Global G2 Root

#	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
18	JoySSL DV Secure Server CA	Signing Key	sha384RSA	3072 bits	CN = JoySSL DV Secure Server CA O = JoySSL Limited C = CN	807B3118B837D850FD1C4AD9879A5E426D00A1A4	AA9CD0737407E9E9D9D86B145A2CFD7CD385C28BCF5996AA8D9A6DA5FC76F3A2	UCA Global G2 Root
19	JoySSL OV Secure Server CA	Signing Key	sha384RSA	3072 bits	CN = JoySSL OV Secure Server CA O = JoySSL Limited C = CN	21507E5079E680B202C0FBC1AFAD8026DC52B8DD	0DD33FA366CA02808D29A5C1C456496AB5015C3604EB21C101406AF2533D998A	UCA Global G2 Root
20	KeepTrust DV TLS RSA CA G1	Signing Key	sha384RSA	3072 bits	CN = KeepTrust DV TLS RSA CA G1 O = Shanghai Huandu Info Tech Co. Ltd. C = CN	5063446A28FAC2B3D5122D01A63D9B85845026CC	A879CB01A2661C255B9C2B9BE0B20BA74EEA9546E21A82C570E177CF5BF4AEDA	UCA Global G2 Root
21	KeepTrust OV TLS RSA CA G1	Signing Key	sha384RSA	3072 bits	CN = KeepTrust OV TLS RSA CA G1 O = Shanghai Huandu Info Tech Co. Ltd. C = CN	04FA1B9DBC05CD575CC6518D5CDFE62CD151B0C8	FFD0D9EEEAAFBB4C44F71392F20A52E0F65896854933139640722DECFC2D4658	UCA Global G2 Root
22	ZoTrus RSA DV SSL CA	Signing Key	sha384RSA	3072 bits	CN = ZoTrus RSA DV SSL CA O = ZoTrus Technology Limited C = CN	7FEF9B0B9EB3F717A576BBC7580209DE731544B7	69C25861236502F0C223443FD851A2FB6ACB745BB814AD72BB2E50867C52C3BB	UCA Global G2 Root
23	ZoTrus RSA OV SSL CA	Signing Key	sha384RSA	3072 bits	CN = ZoTrus RSA OV SSL CA O = ZoTrus Technology Limited C = CN	E92D57AB2A4455799E257937123588FCDF187AC3	219C59CCD06D0210ADCF6E8125700D1578F69A0670A07FD9DDE99E4AC82524CD	UCA Global G2 Root

#	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
24	CT2 DV TLS RSA CA G1	Signing Key	sha384RSA	3072 bits	CN = CT2 DV TLS RSA CA G1 O = Tianyi Security Technology Co., Ltd. C = CN	8955C1DB0608F7A83C51CA3BF98F017B90098A73	4B316EDFC0780286571E430C0A94231B192B45666AF5DEBEE454FE08E4496383	UCA Global G2 Root
25	CT2 OV TLS RSA CA G1	Signing Key	sha384RSA	3072 bits	CN = CT2 OV TLS RSA CA G1 O = Tianyi Security Technology Co., Ltd. C = CN	27937BF574A8AF23A7F29E2B03CFACC7182B2EFA	A263B7CEFD1490D04FD0EC31D9695BAEE480EE861D12124C2BF8EBD8A893652F	UCA Global G2 Root
26	SHECA FREE DV TLS RSA CA G1	Signing Key	sha384RSA	3072 bits	CN = SHECA FREE DV TLS RSA CA G1 O = UniTrust C = CN	F18082839D6BB5C20A6A43C2D584A9F6F3EF2DC9	DFD9FB07A42E81216D6497FBC47BE53D829BBFD6A9188B02D5C8CDE29E01CF5C	UCA Global G2 Root
27	SHECA FREE DV TLS ECC CA G2	Signing Key	sha384RSA	384 bits	CN = SHECA FREE DV TLS ECC CA G2 O = UniTrust C = CN	84BCFE29594A85C0849FF0F21230812BE73F9BBC	81DB88F4CDE7345B0EC140E4A193720163DF9B787FABA0AF5A7EDACE6DC315A6	UCA Global G2 Root
28	SHECA DV TLS ECC CA G6	Signing Key	sha384RSA	384 bits	CN = SHECA DV TLS ECC CA G6 O = UniTrust C = CN	7E44A7C621F5F30E25293C07F288ECC82F7BD482	1F0570E418F9C89E094CB26EDA71B92BED81ACBB446B2300D398DDB739AB7A6C	UCA Global G2 Root
29	SHECA OV TLS ECC CA G6	Signing Key	sha384RSA	384 bits	CN = SHECA OV TLS ECC CA G6 O = UniTrust C = CN	2569CCEFDB564A83BAC15284500F13D86104FEE0	C4DA2C937523D42054FBB4AF694BB90FC7743C910EE048726241BD84C38509D9	UCA Global G2 Root
30	DNSPod DV TLS RSA CA G1	Signing Key	sha384RSA	3072 bits	CN = DNSPod DV TLS RSA CA G1 O = DNSPod, Inc. C = CN	4CF1C77BBB5F991923F8616FD712F9749C5AE55C	A07A7DEFCD1ED23F36D22AC33421F1D973583B12C96CA2496DE724C4494C0CD2	UCA Global G2 Root

#	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
31	DNSPod DV TLS ECC CA G1	Signing Key	sha384RSA	384 bits	CN = DNSPod DV TLS ECC CA G1 O = DNSPod, Inc. C = CN	B9A7EB6345A DB88940892F 8B69930658D A9733CF	AACCD77057271FF5F 605DF8CC5A44397E7 1CCE796EA79B8F1E8 658FC9CD52464	UCA Global G2 Root
32	DNSPod OV TLS RSA CA G1	Signing Key	sha384RSA	3072 bits	CN = DNSPod OV TLS RSA CA G1 O = DNSPod, Inc. C = CN	38C22FB4856 AB84A51911F E53A7FE2BE1 103338F	F36592E33FD869E91 7E33BADE683A4EC2 0809D5C8B493A1427 BA6DC066CB5AE3	UCA Global G2 Root
33	DNSPod OV TLS ECC CA G1	Signing Key	sha384RSA	384 bits	CN = DNSPod OV TLS ECC CA G1 O = DNSPod, Inc. C = CN	586EA657334 43DCE3CED5 DEBF47E000 F0E81B28D	8C4BFF9AE3F079E50 208F84E4DA658AB4 41109686861FFCEE50 D4A8662C2EEA1	UCA Global G2 Root
34	Keymatic Secure Domain RSA CA G1	Signing Key	sha384RSA	3072 bits	CN = Keymatic Secure Domain RSA CA G1 O = PKI(Chongqing) Limited C = CN	8ED096D6E8 A4D935F386E BDA0B592E4 0521B0CBB	F3C9431A163BECE79 562093F0734DF6ED0 5618551CFEE0ABA94 9A77E959D8AAE	UCA Global G2 Root
35	Keymatic Secure Domain ECC CA G1	Signing Key	sha384RSA	384 bits	CN = Keymatic Secure Domain ECC CA G1 O = PKI(Chongqing) Limited C = CN	C1286B590B1 98916D776E6 661E57D4460 812EDDF	B07D2ACA4F29E2449 B5ADB7CCB31C64C43 854044A2DAA2AC83 8788026C684C0C	UCA Global G2 Root
36	Keymatic Secure Business RSA CA G1	Signing Key	sha384RSA	3072 bits	CN = Keymatic Secure Business RSA CA G1 O = PKI(Chongqing) Limited C = CN	5693F449C7E 448C3C3D2BE 86397E333681 63A377	5523644185E21EF943 A505A1C438167DA1F E7B14BEF2D243E53D E8C2B4263EB7	UCA Global G2 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
37	Keymatic Secure Business ECC CA G1	Signing Key	sha384RSA	384 bits	CN = Keymatic Secure Business ECC CA G1 O = PKI(Chongqing) Limited C = CN	23368DE013A9BB36D76A66E1128EDA5F4A3620D5	75C4AF6628E7D01DD369593EFD727E3560ED9DDD67B0432565 5821BD23281A2B	UCA Global G2 Root
38	sslTrus RSA DV TLS CA G2	Signing Key	sha384RSA	3072 bits	CN = sslTrus RSA DV TLS CA G2 O = sslTrus C = CN	DEE386BAC52E630164E0C142943C3202967C6891	B3A5BED750BCE5A08C75E0012B0A6A67954952BC8D12520514CC15CBB0B17039	UCA Global G2 Root
39	sslTrus ECC DV TLS CA G2	Signing Key	sha384RSA	384 bits	CN = sslTrus ECC DV TLS CA G2 O = sslTrus C = CN	624679EBA47FFA4CD98D6FFFDE6D6F7FE49E86E9	32CAA961415106CF471CEA5B15C66464A907C99861A297C359D174624BADB92F	UCA Global G2 Root
40	sslTrus RSA OV TLS CA G2	Signing Key	sha384RSA	3072 bits	CN = sslTrus RSA OV TLS CA G2 O = sslTrus C = CN	0EDFB68948064E10818E3C8108C824BB8B308F62	F0E647B5A2869A3487507A90549AF039896DB8B0F0E7CF92EF3AB567F3EC5E5C	UCA Global G2 Root
41	sslTrus ECC OV TLS CA G2	Signing Key	sha384RSA	384 bits	CN = sslTrus ECC OV TLS CA G2 O = sslTrus C = CN	BEE114C1BEF84DA5E3D4E41FCA0D1F81A90C0FE0	06B7E611243D2901B964FF6D0C53A2DB52BA2E1D41E17D74950E16605D9A2C90	UCA Global G2 Root
42	HTTPS Automation Research RSA DV SSL CA G1	Signing Key	sha384RSA	3072 bits	CN = HTTPS Automation Research RSA DV SSL CA G1 O = Shenzhen Yamu Security Technology Co., Ltd. C = CN	0FB6A84D71E5B1B38F9E72D6BBC06A147FE4D03B	1E426FF0F51EB4C285788B4418D2DAB21097230CED81119BA178A20AB1AABF67	UCA Global G2 Root
43	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	C1AFC65B1E813B0E6146E6AA5341681272ABE9A38D59F7BD1B27B729834A0D9C	Certum Trusted Network CA

#	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
44	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	3DD69C5BE170F943F804D1D31FE8F916C0C0226CDDD7AEA9AA9A0CDFD3474361	Certum Trusted Network CA
45	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	BB61408AED9F530B2EC0545E53BA2C8EBEAA57D9976447DB1663CED4600CD6B7	Certum Trusted Network CA
46	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	BFA95C5DF164B659FA32F6D10564D7170DDE661A853A782E6AB63639433BCB41	Certum Trusted Network CA
47	UCA Extended Validation Root	Root Key	sha256RSA	4096 bits	CN = UCA Extended Validation Root O = UniTrust C = CN	D9743AE4303D0DF712DC7E5A059F1E349AF7E114	D43AF9B35473755C9684FC06D7D8CB70EE5C28E773FB294EB41EE71722924D24	UCA Extended Validation Root
48	SHECA RSA Extended Validation Server CA	Signing Key	sha256RSA	2048 bits	CN = SHECA RSA Extended Validation Server CA O = UniTrust C = CN	3B4B252A77372AFCB97FEDA8BDAF2299FC5DC5F4	4FD6FA527157EEA463689D7A4C2B934EF222279725413893D9847242C85CA9DF	UCA Extended Validation Root
49	SHECA EV Server CA G3	Signing Key	sha256RSA	2048 bits	CN = SHECA EV Server CA G3 O = UniTrust C = CN	54E972FB78669FE5CBF33B8F98465553739C0B84	7EF3F89456CE636557B20C5DFB37F98C253A0B660D2E9E5E7845CAF9C038C7C1	UCA Extended Validation Root
50	SHECA OV Server CA G6	Signing Key	sha256RSA	2048 bits	CN = SHECA OV Server CA G6 O = UniTrust C = CN	FB7DCE4905B420BCFFBF0D8471ADAE0135F961A0	264DF1458FB5EF1FC9DF9F1345E84A6CC1A471CF475AE7598FF52B86713519FB	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
51	SHECA OV Server CA G7	Signing Key	sha256RSA	2048 bits	CN = SHECA OV Server CA G7 O = UniTrust C = CN	A0F344BA17512C7776AB4442C5534B16AB5F0DAA	F6F8BCD413C9733166E85843B468DD36E727152D9A37B15129C0E7648ECEE639	UCA Extended Validation Root
52	SHECA Extended Validation SSL CA	Signing Key	sha256RSA	2048 bits	CN = SHECA Extended Validation SSL CA O = UniTrust C = CN	4D140DEA6B559C0CA6E1BB7BE86A966D175E7CB5	25BFDB1C5FE2CCE051EC6DFBF2BB24E78C92F969B1BB37867DAEDF93D1A7AE7E	UCA Extended Validation Root
53	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
54	SHECA DV Server CA 1A	Signing Key	sha384RSA	4096 bits	CN = SHECA DV Server CA 1A O = UniTrust C = CN	653740E0BBF43905206A8C9CA0ACB3BBD6968CA0	D3D4A040BB41A695A96E3AAD93814CF7EF219D5819206E947B44DCC5B8E5E272	UniTrust Global Root CA R1
55	SHECA OV Server CA 1A	Signing Key	sha384RSA	4096 bits	CN = SHECA OV Server CA 1A O = UniTrust C = CN	8CD02E82008EE2DEFF71F61A105C74A826E858D1	9A3DB0F0FB0FF4F974A4E0C510A7C13D350485B1E6CDF5A899BB24D0F499E9BD	UniTrust Global Root CA R1
56	SHECA EV Server CA 1A	Signing Key	sha384RSA	4096 bits	CN = SHECA EV Server CA 1A O = UniTrust C = CN	73E36DF62D862F57DF69A53687231C85E0170216	2F1CA1A5C0D7AE58C7ADFC69D4C57EE815F39C0F3D1F982E3AC76D25AB723995	UniTrust Global Root CA R1

#	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
57	UniTrust Global Root CA R2	Root Key	sha384ECDSA	384 bits	CN = UniTrust Global Root CA R2 O = UniTrust C = CN	E45366B7B7A4E9D7CCC121E04ACFCCAC01BC72BC	78919B35D1C615595A51328A5C546083B4D5320724A258695B991F2F61C4DCC7	UniTrust Global Root CA R2
58	SHECA DV Server CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA DV Server CA 2A O = UniTrust C = CN	A1221170BEC8665F6ECB104C4EDB38EA9C1F914D	69201DC24E4127FFA5B41A0DDF0A1A005C00F334B003F1008924CBF998E1827C	UniTrust Global Root CA R2
59	SHECA OV Server CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA OV Server CA 2A O = UniTrust C = CN	98CDEC338767F39422373810B735BA7C683A8259	8E2CA2825C2039804A7A1CC54B002EA1DB30AC489698F039527BF1602132F611	UniTrust Global Root CA R2
60	SHECA EV Server CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA EV Server CA 2A O = UniTrust C = CN	44661C71EF69B7930AB5B771D83B114CFA843D77	93E49170D20F54DA701118A5ABDCDDA4FFCF334CDB2D8D80599AB62848C85F80	UniTrust Global Root CA R2
61	UniTrust Global TLS ECC Root CA R2	Root Key	sha384ECDSA	384 bits	CN = UniTrust Global TLS ECC Root CA R2 O = UniTrust C = CN	7935AD798A95305C3E05A675161A97000F6FCC90	6C689FC6B014A1FB0CDEB5A3996171C15E72861060285 32E0210CEA8D9CD4E97	UniTrust Global TLS ECC Root CA R2
62	SHECA DV TLS ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA DV TLS ECC CA 2A O = UniTrust C = CN	CB65E62F50175F2C172B433F3A043CD213569A66	D690D8722EA89CD761790144952065333 9386AC4939F7EC5C1B195D9C3C95FA4	UniTrust Global TLS ECC Root CA R2

#	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
63	SHECA EV TLS ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA EV TLS ECC CA 2A O = UniTrust C = CN	B353900B5E40A4952EA85A27F413ABBAD631F233	05E4C4B1F258030690E6793C9C13C6F6AE234F68E5C41236FDC919B7F589032F	UniTrust Global TLS ECC Root CA R2
64	SHECA OV TLS ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA OV TLS ECC CA 2A O = UniTrust C = CN	A065578C43B2546C4E18DF86AED56725A9B7659C	08BA64405A3406C97BDCBD0E44224E6DD341F3EC93F1368457DFA7CAC88BE150	UniTrust Global TLS ECC Root CA R2
65	UniTrust Global TLS RSA Root CA R1	Root Key	sha384RSA	4096 bits	CN = UniTrust Global TLS RSA Root CA R1 O = UniTrust C = CN	F2ADBFAB6708F09672E633D65175A24759C900C4	4BABE0E9328D5DAE17936F3DDAA2442BFBDD0873F92FB8D1FBBD3D9894649AD9	UniTrust Global TLS RSA Root CA R1
66	SHECA DV TLS RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA DV TLS RSA CA 1A O = UniTrust C = CN	C5E3A87F7EEDBC3E7108B34EF490EF2F2F1367D1	FFABEA74895DC0C78C224597472CF6937E0D740EF49DC2256C8E75A2A2A15EDE	UniTrust Global TLS RSA Root CA R1
67	SHECA EV TLS RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA EV TLS RSA CA 1A O = UniTrust C = CN	60651A135EAB2B98A5A1041B3057A1D02FC612E5	B2525A5966CA68CA7F504F0A21FD73847D174F89B48852A3E970588E1EAFC774	UniTrust Global TLS RSA Root CA R1
68	SHECA OV TLS RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA OV TLS RSA CA 1A O = UniTrust C = CN	F463091C1E2788B75DBBE91644B1744A34F34B46	7F8EF707C2D9A4B7D4ED5FDDC8AF4A64D99BF297D03F8F01C4375DE74B1C7DE1	UniTrust Global TLS RSA Root CA R1

附录 B – 公开披露的事件

下表列示了 2024 年 4 月 1 日至 2025 年 3 月 31 日期间本报告范围内的公开披露事件：

Bugzilla ID	**事件名称**	**事件链接**
1902592	SHECA: EV certificate subject RDN order is incorrect	Bugzilla Ticket Link
1902947	SHECA: The certificate's cpsURI is empty	Bugzilla Ticket Link
1914365	SHECA: CRLReason code usage error	Bugzilla Ticket Link
1946921	SHECA: DV SSL certificate format is abnormal	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

9 May 2025

Dear Sirs,

Assertion of Management as to the Disclosure of Business Practices and Controls over the Certification Authority - SSL Operations during the period from April 1, 2024 through March 31, 2025

Shanghai Electronic Certificate Authority Co., Ltd. ("SHECA") operates the Certification Authority (CA) services known as its Root and Subordinate CAs (please refer to the Attachment A) for SSL Baseline Requirements and provides SSL CA services.

The management of SHECA is responsible for establishing and maintaining effective controls over its SSL CA operations, including its SSL CA business practices disclosure on its website, SSL key lifecycle management controls, and SSL certificate lifecycle management controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error, and the circumvention or overriding of controls. Accordingly, even effective controls can only provide reasonable assurance with respect to SHECA's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

SHECA management has assessed its disclosures of its certificate practices and controls over its 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 April 1, 2024 to March 31, 2025, SHECA has:

- disclosed its SSL certificate lifecycle management business practices in its:
  - UniTrust Certification Practice Statement v3.7.9;
  - UniTrust Certification Practice Statement v3.7.8;
  - UniTrust Certification Practice Statement v3.7.7;
  - UniTrust Certificate Policy v1.5.7;
  - UniTrust Certificate Policy v1.5.6; and
  - UniTrust Certificate Policy v1.5.5

  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

in accordance with the WebTrust Principles and Criteria for Certification Authorities - SSL Baseline v2.8.

The UniTrust Global Root CA R1 (Attachment A #53), UniTrust Global Root CA R2 (Attachment A #57), UniTrust Global TLS ECC Root CA R2 (Attachment A #61), and UniTrust Global TLS RSA Root CA R1 (Attachment A #65) CAs did not issue certificates during the period April 1, 2024 to March 31, 2025 and were maintained online to provide revocation status information only.

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

Company Chop

Attachment 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	9BEA11C976FE014764C1BE56A6F914B5A5600317ABD9988393382E5161AA0493C	UCA Global G2 Root
2	SHECA RSA Domain Validation Server CA G3	Signing Key	sha256RSA	2048 bits	CN = SHECA RSA Domain Validation Server CA G3 O = UniTrust C = CN	057A4D756FFD0A83B1671675773E14C5F53C548E	0A552A65F22FF820E7EC3D43BBF88B02ABC34BD247E0C3505891B6342F16A5F2	UCA Global G2 Root
3	SHECA RSA Organization Validation Server CA G3	Signing Key	sha256RSA	2048 bits	CN = SHECA RSA Organization Validation Server CA G3 O = UniTrust C = CN	316068091E32F9F6CCC06215AA7B91AF4C119D40	26FD4C4367E463D39C71796AE4010E53380DC93BC132FB019D6718A6873E81F4	UCA Global G2 Root
4	SHECA DV Server CA G5	Signing Key	sha256RSA	2048 bits	CN = SHECA DV Server CA G5 O = UniTrust C = CN	D8E7061B645FAB3008887A2453AAE11C8304BF6D	778C516DAEC700EE58B3581E411E5C0DD478663A5163A29895341507D6E964DD	UCA Global G2 Root
5	SHECA OV Server CA G5	Signing Key	sha256RSA	2048 bits	CN = SHECA OV Server CA G5 O = UniTrust C = CN	0379A38D525FD4E988921F4358542502F4878B7E	8AB3A0ACF289E6EF754BE449236843D67F45C191BDDD66484B85E6E60556A9AF	UCA Global G2 Root
6	SHECA EV Server CA G2	Signing Key	sha256RSA	2048 bits	CN = SHECA EV Server CA G2 O = UniTrust C = CN	86B148C0420A9C6F81FC4FDCD10F184BAAB5A6EA	4216527163AD2CAA825D3BF48F61A7661D0ABC89B58AB76B23A1E10999F0769F	UCA Global G2 Root
7	TrustAsia RSA DV TLS CA - S1	Signing Key	sha256RSA	2048 bits	CN = TrustAsia RSA DV TLS CA - S1 O = TrustAsia Technologies, Inc. C = CN	9432E0D48ACD1D93E75C5372960C5EF1F3F67972	074ADD7F1E73EB110EC8E2B78A92C51CF5A451135B6F7DEFC019EE9D74BFA4D6	UCA Global G2 Root
8	TrustAsia RSA OV TLS CA - S1	Signing Key	sha256RSA	2048 bits	CN = TrustAsia RSA OV TLS CA - S1 O = TrustAsia Technologies, Inc. C = CN	F575D48E293E17A8A9C49EDCE6DB0A344D132AEB	D16BA9ACB74FEE4AA8087EE482E86E7F6F5F55FAC5025639730753FE1E705E3C	UCA Global G2 Root
9	SHECA Global G3 SSL	Signing Key	sha256RSA	2048 bits	CN = SHECA Global G3 SSL O = UniTrust S = Shanghai C = CN	9820F0F1D942A6DE833F991019003D6868D20181	AEFFE4335EE56422E927F45E95AE142B9EB35979A7400569AE9BDEA6CAABC1DC	UCA Global G2 Root

#	Key Name	Key Type	Signature Algorithm	Key Size	Subject DN	Subject Key Identifier	Certificates Thumbprint (SHA256)	Certificate Signed by
10	Xinnet DV SSL	Signing Key	sha256RSA	2048 bits	CN = Xinnet DV SSL O = 北京新网数码信息技术有限公司 C = CN	9D3AA5B8E2212783643FF578DC22B04E6BCB36D4	9C53902F9501F6D89766999DBE2AD1A1436420B652535CDC2DC51CCFE2FFEE68	UCA Global G2 Root
11	Xinnet OV SSL	Signing Key	sha256RSA	2048 bits	CN = Xinnet OV SSL O = 北京新网数码信息技术有限公司 C = CN	4B78C0324A2442784E9F83F0D0FE336C7E0D934F	3C07D7EFC8D458F668C10D4F06F90503CCD25D59E2B3F1D58B32884D9E4E3809	UCA Global G2 Root
12	JoySSL DV Secure Server CA G1	Signing Key	sha384RSA	3072 bits	CN = JoySSL DV Secure Server CA G1 O = JoySSL Limited C = CN	2A56E8EF40E0A9999D6DD8129FB79B056B882DED	AA9CD0737407E9E9D9D86B145A2CFD7CD385C28BCF5996AA8D9A6DA5FC76F3A2	UCA Global G2 Root
13	JoySSL OV Secure Server CA G1	Signing Key	sha384RSA	3072 bits	CN = JoySSL OV Secure Server CA G1 O = JoySSL Limited C = CN	6BF2449C86D0C6DED85107661B2748792342CB95	0DD33FA366CA02808D29A5C1C456496AB5015C3604EB21C101406AF2533D998A	UCA Global G2 Root
14	KeepTrust DV TLS RSA CA G2	Signing Key	sha384RSA	3072 bits	CN = KeepTrust DV TLS RSA CA G2 O = Shanghai Huandu Info Tech Co. Ltd. C = CN	088B0DF30B0966297021D02C377300F5A7F4E7E9	352582CCC85B3944E3CD2505D9318F22ABEA418BFF29A0FE4D2C0DF280F200E3	UCA Global G2 Root
15	KeepTrust OV TLS RSA CA G2	Signing Key	sha384RSA	3072 bits	CN = KeepTrust OV TLS RSA CA G2 O = Shanghai Huandu Info Tech Co. Ltd. C = CN	F68D3850B96EA8BEFC50CA91247F1ABC9EA39D4D	CD50559A6DC5C704237EABF9A070B79F0CDFC1A79C3A6AC8C5E71E295A065D0A	UCA Global G2 Root
16	ZoTrus RSA DV SSL CA G1	Signing Key	sha384RSA	3072 bits	CN = ZoTrus RSA DV SSL CA G1 O = ZoTrus Technology Limited C = CN	EC1EBCB71E092769EFA715E89AA1677C33AA0F5A	E7EF1AD946214B32AF03CC287930D0464ED2C086D7A1447C6E27FC9217D4E16B	UCA Global G2 Root
17	ZoTrus RSA OV SSL CA G1	Signing Key	sha384RSA	3072 bits	CN = ZoTrus RSA OV SSL CA G1 O = ZoTrus Technology Limited C = CN	A0FA64A37EB83C7C194C51B7FE6A2BE8A39F78A4	3EC123D71DB27AE1DC8F877286C222F4167A2AE4FD7BCF370789EF4A9521B8	UCA Global G2 Root
18	JoySSL DV Secure Server CA	Signing Key	sha384RSA	3072 bits	CN = JoySSL DV Secure Server CA O = JoySSL Limited C = CN	807B3118B837D850FD1C4AD9879A5E426D00A1A4	AA9CD0737407E9E9D9D86B145A2CFD7CD385C28BCF5996AA8D9A6DA5FC76F3A2	UCA Global G2 Root

#	Key Name	Key Type	Signature Algorithm	Key Size	Subject DN	Subject Key Identifier	Certificates Thumbprint (SHA256)	Certificate Signed by
19	JoySSL OV Secure Server CA	Signing Key	sha384RSA	3072 bits	CN = JoySSL OV Secure Server CA O = JoySSL Limited C = CN	21507E5079E680B202C0FBC1AFAD8026DC52B8DD	0DD33FA366CA02808D29A5C1C456496AB5015C3604EB21C101406AF2533D998A	UCA Global G2 Root
20	KeepTrust DV TLS RSA CA G1	Signing Key	sha384RSA	3072 bits	CN = KeepTrust DV TLS RSA CA G1 O = Shanghai Huandu Info Tech Co. Ltd. C = CN	5063446A28FAC2B3D5122D01A63D9B85845026CC	A879CB01A2661C255B9C2B9BE0B20BA74EEA9546E21A82C570E177CF5BF4AEDA	UCA Global G2 Root
21	KeepTrust OV TLS RSA CA G1	Signing Key	sha384RSA	3072 bits	CN = KeepTrust OV TLS RSA CA G1 O = Shanghai Huandu Info Tech Co. Ltd. C = CN	04FA1B9DBC05CD575CC6518D5CDFE62CD151B0C8	FFD0D9EEEAAFBB4C44F71392F20A52E0F65896854933139640722DECFC2D4658	UCA Global G2 Root
22	ZoTrus RSA DV SSL CA	Signing Key	sha384RSA	3072 bits	CN = ZoTrus RSA DV SSL CA O = ZoTrus Technology Limited C = CN	7FEF9B0B9EB3F717A576BBC7580209DE731544B7	69C25861236502F0C223443FD851A2FB6ACB745BB814AD72BB2E50867C52C3BB	UCA Global G2 Root
23	ZoTrus RSA OV SSL CA	Signing Key	sha384RSA	3072 bits	CN = ZoTrus RSA OV SSL CA O = ZoTrus Technology Limited C = CN	E92D57AB2A4455799E257937123588FCDF187AC3	219C59CCD06D0210ADCF6E8125700D1578F69A0670A07FD9DDE99E4AC82524CD	UCA Global G2 Root
24	CT2 DV TLS RSA CA G1	Signing Key	sha384RSA	3072 bits	CN = CT2 DV TLS RSA CA G1 O = Tianyi Security Technology Co., Ltd. C = CN	8955C1DB0608F7A83C51CA3BF98F017B90098A73	4B316EDFC0780286571E430C0A94231B192B45666AF5DEBEE454FE08E4496383	UCA Global G2 Root
25	CT2 OV TLS RSA CA G1	Signing Key	sha384RSA	3072 bits	CN = CT2 OV TLS RSA CA G1 O = Tianyi Security Technology Co., Ltd. C = CN	27937BF574A8AF23A7F29E2B03CFACC7182B2EFA	A263B7CEFD1490D04FD0EC31D9695BAEE480EE861D12124C2BF8EBD8A893652F	UCA Global G2 Root
26	SHECA FREE DV TLS RSA CA G1	Signing Key	sha384RSA	3072 bits	CN = SHECA FREE DV TLS RSA CA G1 O = UniTrust C = CN	F18082839D6BB5C20A6A43C2D584A9F6F3EF2DC9	DFD9FB07A42E81216D6497FBC47BE53D829BBFD6A9188B02D5C8CDE29E01CF5C	UCA Global G2 Root

#	Key Name	Key Type	Signature Algorithm	Key Size	Subject DN	Subject Key Identifier	Certificates Thumbprint (SHA256)	Certificate Signed by
27	SHECA FREE DV TLS ECC CA G2	Signing Key	sha384RSA	384 bits	CN = SHECA FREE DV TLS ECC CA G2 O = UniTrust C = CN	84BCFE29594A85C0849FF0F21230812BE73F9BBC	81DB88F4CDE7345B0EC140E4A193720163DF9B787FABA0AF5A7EDACE6DC315A6	UCA Global G2 Root
28	SHECA DV TLS ECC CA G6	Signing Key	sha384RSA	384 bits	CN = SHECA DV TLS ECC CA G6 O = UniTrust C = CN	7E44A7C621F5F30E25293C07F288ECC82F7BD482	1F0570E418F9C89E094CB26EDA71B92BED81ACBB446B2300D398DDB739AB7A6C	UCA Global G2 Root
29	SHECA OV TLS ECC CA G6	Signing Key	sha384RSA	384 bits	CN = SHECA OV TLS ECC CA G6 O = UniTrust C = CN	2569CCEFDB564A83BAC15284500F13D86104FEE0	C4DA2C937523D42054FBB4AF694BB90FC7743C910EE048726241BD84C38509D9	UCA Global G2 Root
30	DNSPod DV TLS RSA CA G1	Signing Key	sha384RSA	3072 bits	CN = DNSPod DV TLS RSA CA G1 O = DNSPod, Inc. C = CN	4CF1C77BBB5F991923F8616FD712F9749C5AE55C	A07A7DEFCD1ED23F36D22AC33421F1D973583B12C96CA2496DE724C4494C0CD2	UCA Global G2 Root
31	DNSPod DV TLS ECC CA G1	Signing Key	sha384RSA	384 bits	CN = DNSPod DV TLS ECC CA G1 O = DNSPod, Inc. C = CN	B9A7EB6345ADB88940892F8B69930658DA9733CF	AACCD77057271FF5F605DF8CC5A44397E71CCE796EA79B8F1E8658FC9CD52464	UCA Global G2 Root
32	DNSPod OV TLS RSA CA G1	Signing Key	sha384RSA	3072 bits	CN = DNSPod OV TLS RSA CA G1 O = DNSPod, Inc. C = CN	38C22FB4856AB84A51911FE53A7FE2BE1103338F	F36592E33FD869E917E33BADE683A4EC20809D5C8B493A1427BA6DC066CB5AE3	UCA Global G2 Root
33	DNSPod OV TLS ECC CA G1	Signing Key	sha384RSA	384 bits	CN = DNSPod OV TLS ECC CA G1 O = DNSPod, Inc. C = CN	586EA65733443DCE3CED5DEBF47E000F0E81B28D	8C4BFF9AE3F079E50208F84E4DA658AB441109686861FFCEE50D4A8662C2EEA1	UCA Global G2 Root
34	Keymatic Secure Domain RSA CA G1	Signing Key	sha384RSA	3072 bits	CN = Keymatic Secure Domain RSA CA G1 O = PKI(Chongqing) Limited C = CN	8ED096D6E8A4D935F386EBDA0B592E40521B0CBB	F3C9431A163BECE79562093F0734DF6ED05618551CFEE0ABA949A77E959D8AAE	UCA Global G2 Root
35	Keymatic Secure Domain ECC CA G1	Signing Key	sha384RSA	384 bits	CN = Keymatic Secure Domain ECC CA G1 O = PKI(Chongqing) Limited C = CN	C1286B590B198916D776E6661E57D4460812EDDF	B07D2ACA4F29E2449B5ADB7CCB31C64C43854044A2DAA2AC838788026C684C0C	UCA Global G2 Root
36	Keymatic Secure Business RSA CA G1	Signing Key	sha384RSA	3072 bits	CN = Keymatic Secure Business RSA CA G1 O = PKI(Chongqing) Limited C = CN	5693F449C7E448C3C3D2BE86397E33368163A377	5523644185E21EF943A505A1C438167DA1FE7B14BEF2D243E53DE8C2B4263EB7	UCA Global G2 Root

#	Key Name	Key Type	Signature Algorithm	Key Size	Subject DN	Subject Key Identifier	Certificates Thumbprint (SHA256)	Certificate Signed by
37	Keymatic Secure Business ECC CA G1	Signing Key	sha384RSA	384 bits	CN = Keymatic Secure Business ECC CA G1 O = PKI(Chongqing) Limited C = CN	23368DE013A9BB36D76A66E1128EDA5F4A3620D5	75C4AF6628E7D01DD369593EFD727E3560ED9DDD67B04325655821BD23281A2B	UCA Global G2 Root
38	sslTrus RSA DV TLS CA G2	Signing Key	sha384RSA	3072 bits	CN = sslTrus RSA DV TLS CA G2 O = sslTrus C = CN	DEE386BAC52E630164E0C142943C3202967C6891	B3A5BED750BCE5A08C75E0012B0A6A67954952BC8D12520514CC15CBB0B17039	UCA Global G2 Root
39	sslTrus ECC DV TLS CA G2	Signing Key	sha384RSA	384 bits	CN = sslTrus ECC DV TLS CA G2 O = sslTrus C = CN	624679EBA47FFA4CD98D6FFFDE6D6F7FE49E86E9	32CAA961415106CF471CEA5B15C66464A907C99861A297C359D174624BADB92F	UCA Global G2 Root
40	sslTrus RSA OV TLS CA G2	Signing Key	sha384RSA	3072 bits	CN = sslTrus RSA OV TLS CA G2 O = sslTrus C = CN	0EDFB68948064E10818E3C8108C824BB8B308F62	F0E647B5A2869A3487507A90549AF039896DB8B0F0E7CF92EF3AB567F3EC5E5C	UCA Global G2 Root
41	sslTrus ECC OV TLS CA G2	Signing Key	sha384RSA	384 bits	CN = sslTrus ECC OV TLS CA G2 O = sslTrus C = CN	BEE114C1BEF84DA5E3D4E41FCA0D1F81A90C0FE0	06B7E611243D2901B964FF6D0C53A2DB52BA2E1D41E17D74950E16605D9A2C90	UCA Global G2 Root
42	HTTPS Automation Research RSA DV SSL CA G1	Signing Key	sha384RSA	3072 bits	CN = HTTPS Automation Research RSA DV SSL CA G1 O = Shenzhen Yamu Security Technology Co., Ltd. C = CN	0FB6A84D71E5B1B38F9E72D6BBC06A147FE4D03B	1E426FF0F51EB4C285788B4418D2DAB21097230CED81119BA178A20AB1AABF67	UCA Global G2 Root
43	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	C1AFC65B1E813B0E6146E6AA5341681272ABE9A38D59F7BD1B27B729834A0D9C	Certum Trusted Network CA
44	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	3DD69C5BE170F943F804D1D31FE8F916C0C0226CDDD7AEA9AA9A0CDFD3474361	Certum Trusted Network CA
45	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	BB61408AED9F530B2EC0545E53BA2C8EBEAA57D9976447DB1663CED4600CD6B7	Certum Trusted Network CA
46	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	BFA95C5DF164B659FA32F6D10564D7170DDE661A853A782E6AB63639433BCB41	Certum Trusted Network CA
47	UCA Extended Validation Root	Root Key	sha256RSA	4096 bits	CN = UCA Extended Validation Root O = UniTrust C = CN	D9743AE4303D0DF712DC7E5A059F1E349AF7E114	D43AF9B35473755C9684FC06D7D8CB70EE5C28E773FB294EB41EE71722924D24	UCA Extended Validation Root

#	Key Name	Key Type	Signature Algorithm	Key Size	Subject DN	Subject Key Identifier	Certificates Thumbprint (SHA256)	Certificate Signed by
48	SHECA RSA Extended Validation Server CA	Signing Key	sha256RSA	2048 bits	CN = SHECA RSA Extended Validation Server CA O = UniTrust C = CN	3B4B252A77372AFCB97FEDA8BDAF2299FC5DC5F4	4FD6FA527157EEA463689D7A4C2B934EF222279725413893D9847242C85CA9DF	UCA Extended Validation Root
49	SHECA EV Server CA G3	Signing Key	sha256RSA	2048 bits	CN = SHECA EV Server CA G3 O = UniTrust C = CN	54E972FB78669FE5CBF33B8F98465553739C0B84	7EF3F89456CE636557B20C5DFB37F98C253A0B660D2E9E5E7845CAF9C038C7C1	UCA Extended Validation Root
50	SHECA OV Server CA G6	Signing Key	sha256RSA	2048 bits	CN = SHECA OV Server CA G6 O = UniTrust C = CN	FB7DCE4905B420BCFFBF0D8471ADAE0135F961A0	264DF1458FB5EF1FC9DF9F1345E84A6CC1A471CF475AE7598FF52B86713519FB	UCA Extended Validation Root
51	SHECA OV Server CA G7	Signing Key	sha256RSA	2048 bits	CN = SHECA OV Server CA G7 O = UniTrust C = CN	A0F344BA17512C7776AB4442C5534B16AB5F0DAA	F6F8BCD413C9733166E85843B468DD36E727152D9A37B15129C0E7648ECEE639	UCA Extended Validation Root
52	SHECA Extended Validation SSL CA	Signing Key	sha256RSA	2048 bits	CN = SHECA Extended Validation SSL CA O = UniTrust C = CN	4D140DEA6B559C0CA6E1BB7BE86A966D175E7CB5	25BFDB1C5FE2CCE051EC6DFBF2BB24E78C92F969B1BB37867DAEDF93D1A7AE7E	UCA Extended Validation Root
53	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
54	SHECA DV Server CA 1A	Signing Key	sha384RSA	4096 bits	CN = SHECA DV Server CA 1A O = UniTrust C = CN	653740E0BBF43905206A8C9CA0ACB3BBD6968CA0	D3D4A040BB41A695A96E3AAD93814CF7EF219D5819206E947B44DCC5B8E5E272	UniTrust Global Root CA R1
55	SHECA OV Server CA 1A	Signing Key	sha384RSA	4096 bits	CN = SHECA OV Server CA 1A O = UniTrust C = CN	8CD02E82008EE2DEFF71F61A105C74A826E858D1	9A3DB0F0FB0FF4F974A4E0C510A7C13D350485B1E6CDF5A899BB24D0F499E9BD	UniTrust Global Root CA R1
56	SHECA EV Server CA 1A	Signing Key	sha384RSA	4096 bits	CN = SHECA EV Server CA 1A O = UniTrust C = CN	73E36DF62D862F57DF69A53687231C85E0170216	2F1CA1A5C0D7AE58C7ADFC69D4C57EE815F39C0F3D1F982E3AC76D25AB723995	UniTrust Global Root CA R1
57	UniTrust Global Root CA R2	Root Key	sha384ECDSA	384 bits	CN = UniTrust Global Root CA R2 O = UniTrust C = CN	E45366B7B7A4E9D7CCC121E04ACFCCAC01BC72BC	78919B35D1C615595A51328A5C546083B4D5320724A258695B991F2F61C4DCC7	UniTrust Global Root CA R2
58	SHECA DV Server CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA DV Server CA 2A O = UniTrust C = CN	A1221170BEC8665F6ECB104C4EDB38EA9C1F914D	69201DC24E4127FFA5B41A0DDF0A1A005C00F334B003F1008924CBF998E1827C	UniTrust Global Root CA R2

#	Key Name	Key Type	Signature Algorithm	Key Size	Subject DN	Subject Key Identifier	Certificates Thumbprint (SHA256)	Certificate Signed by
59	SHECA OV Server CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA OV Server CA 2A O = UniTrust C = CN	98CDEC338767F3942237381 0B735BA7C683A8259	8E2CA2825C2039804A7A1CC54B002EA1DB30AC489698F039527BF1602132F611	UniTrust Global Root CA R2
60	SHECA EV Server CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA EV Server CA 2A O = UniTrust C = CN	44661C71EF69B7930AB5B771D83B114CFA843D77	93E49170D20F54DA701118A5ABDCDDA4FFCF334CDB2D8D80599AB62848C85F80	UniTrust Global Root CA R2
61	UniTrust Global TLS ECC Root CA R2	Root Key	sha384ECDSA	384 bits	CN = UniTrust Global TLS ECC Root CA R2 O = UniTrust C = CN	7935AD798A95305C3E05A675161A97000F6FCC90	6C689FC6B014A1FB0CDEB5A3996171C15E7286106028532E0210CEA8D9CD4E97	UniTrust Global TLS ECC Root CA R2
62	SHECA DV TLS ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA DV TLS ECC CA 2A O = UniTrust C = CN	CB65E62F50175F2C172B433F3A043CD213569A66	D690D8722EA89CD761790144952065333 9386AC4939F7EC5C1B195D9C3C95FA4	UniTrust Global TLS ECC Root CA R2
63	SHECA EV TLS ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA EV TLS ECC CA 2A O = UniTrust C = CN	B353900B5E40A4952EA85A27F413ABBAD631F233	05E4C4B1F258030690E6793C9C13C6F6AE234F68E5C41236FDC919B7F589032F	UniTrust Global TLS ECC Root CA R2
64	SHECA OV TLS ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA OV TLS ECC CA 2A O = UniTrust C = CN	A065578C43B2546C4E18DF86AED56725A9B7659C	08BA64405A3406C97BDCBD0E44224E6DD341F3EC93F1368457DFA7CAC88BE150	UniTrust Global TLS ECC Root CA R2
65	UniTrust Global TLS RSA Root CA R1	Root Key	sha384RSA	4096 bits	CN = UniTrust Global TLS RSA Root CA R1 O = UniTrust C = CN	F2ADBFAB6708F09672E633D65175A24759C900C4	4BABE0E9328D5DAE17936F3DDAA2442BFBDD0873F92FB8D1FBBD3D9894649AD9	UniTrust Global TLS RSA Root CA R1
66	SHECA DV TLS RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA DV TLS RSA CA 1A O = UniTrust C = CN	C5E3A87F7EEDBC3E7108B34EF490EF2F2F1367D1	FFABEA74895DC0C78C224597472CF6937E0D740EF49DC2256C8E75A2A2A15EDE	UniTrust Global TLS RSA Root CA R1
67	SHECA EV TLS RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA EV TLS RSA CA 1A O = UniTrust C = CN	60651A135EAB2B98A5A1041B3057A1D02FC612E5	B2525A5966CA68CA7F504F0A21FD73847D174F89B48852A3E970588E1EAFC774	UniTrust Global TLS RSA Root CA R1
68	SHECA OV TLS RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA OV TLS RSA CA 1A O = UniTrust C = CN	F463091C1E2788B75DBBE91644B1744A34F34B46	7F8EF707C2D9A4B7D4ED5FDDC8AF4A64D99BF297D03F8F01C4375DE74B1C7DE1	UniTrust Global TLS RSA Root CA R1

上海市数字证书认证中心有限公司

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

罗兵咸永道会计师事务所
香港中环太子大厦22楼

2025 年 5 月 9 日

致：罗兵咸永道会计师事务所

就 2024 年 4 月 1 日到 2025 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 SSL 电子认证服务建立并维护有效的控制，包括：披露 SSL 电子认证业务规则，SSL 密钥生命周期管理，SSL 证书生命周期管理。这些控制包括监控机制及为纠正已识别的缺陷所采取的改进措施。

任何控制都有其固有限制，包括人为失误，以及规避或逾越控制的可能性。因此，即使有效的控制也仅能对 SHECA 运营的电子认证服务提供合理保证。此外，由于控制环境的变化，控制的有效性可能随时间而发生变化。

SHECA 管理层已对证书业务披露和 SSL 电子认证服务控制进行评估。基于此评估，在 2024 年 4 月 1 日至 2025 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 v3.7.9；
  - UniTrust证书认证业务规则v3.7.8；
  - UniTrust证书认证业务规则 v3.7.7；
  - UniTrust证书策略 v1.5.7；
  - UniTrust证书策略 v1.5.6；以及
  - UniTrust证书策略 v1.5.5，

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，

以符合 WebTrust电子认证SSL基准规范审计标准 v2.8。

UniTrust Global Root CA R1（附录 A#53），UniTrust Global Root CA R2（附录 A#57），UniTrust Global TLS ECC Root CA R2（附录 A#61）和 UniTrust Global TLS RSA Root CA R1（附录 A#65）在 2024 年 4 月 1 日至 2025 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 Domain Validation Server CA G3	Signing Key	sha256RSA	2048 bits	CN = SHECA RSA Domain Validation Server CA G3 O = UniTrust C = CN	057A4D756FFD0A83B1671675773E14C5F53C548E	0A552A65F22FF820E7EC3D43BBF88B02ABC34BD247E0C3505891B6342F16A5F2	UCA Global G2 Root
3	SHECA RSA Organization Validation Server CA G3	Signing Key	sha256RSA	2048 bits	CN = SHECA RSA Organization Validation Server CA G3 O = UniTrust C = CN	316068091E32F9F6CCC06215AA7B91AF4C119D40	26FD4C4367E463D39C71796AE4010E53380DC93BC132FB019D6718A6873E81F4	UCA Global G2 Root
4	SHECA DV Server CA G5	Signing Key	sha256RSA	2048 bits	CN = SHECA DV Server CA G5 O = UniTrust C = CN	D8E7061B645FAB3008887A2453AAE11C8304BF6D	778C516DAEC700EE58B3581E411E5C0DD478663A5163A29895341507D6E964DD	UCA Global G2 Root
5	SHECA OV Server CA G5	Signing Key	sha256RSA	2048 bits	CN = SHECA OV Server CA G5 O = UniTrust C = CN	0379A38D525FD4E988921F4358542502F4878B7E	8AB3A0ACF289E6EF754BE449236843D67F45C191BDDD66484B85E6E60556A9AF	UCA Global G2 Root
6	SHECA EV Server CA G2	Signing Key	sha256RSA	2048 bits	CN = SHECA EV Server CA G2 O = UniTrust C = CN	86B148C0420A9C6F81FC4FDCD10F184BAAB5A6EA	4216527163AD2CAA825D3BF48F61A7661D0ABC89B58AB76B23A1E10999F0769F	UCA Global G2 Root

#	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	TrustAsia RSA DV TLS CA - S1	Signing Key	sha256RSA	2048 bits	CN = TrustAsia RSA DV TLS CA - S1 O = TrustAsia Technologies, Inc. C = CN	9432E0D48ACD1D93E75C5372960C5EF1F3F67972	074ADD7F1E73EB110EC8E2B78A92C51CF5A451135B6F7DEFC019EE9D74BFA4D6	UCA Global G2 Root
8	TrustAsia RSA OV TLS CA - S1	Signing Key	sha256RSA	2048 bits	CN = TrustAsia RSA OV TLS CA - S1 O = TrustAsia Technologies, Inc. C = CN	F575D48E293E17A8A9C49EDCE6DB0A344D132AEB	D16BA9ACB74FEE4AA8087EE482E86E7F6F5F55FAC5025639730753FE1E705E3C	UCA Global G2 Root
9	SHECA Global G3 SSL	Signing Key	sha256RSA	2048 bits	CN = SHECA Global G3 SSL O = UniTrust S = Shanghai C = CN	9820F0F1D942A6DE833F991019003D6868D20181	AEFFE4335EE56422E927F45E95AE142B9EB35979A7400569AE9BDEA6CAABC1DC	UCA Global G2 Root
10	Xinnet DV SSL	Signing Key	sha256RSA	2048 bits	CN = Xinnet DV SSL O = 北京新网数码信息技术有限公司 C = CN	9D3AA5B8E2212783643FF578DC22B04E6BCB36D4	9C53902F9501F6D89766999DBE2AD1A1436420B652535CDC2DC51CCFE2FFEE68	UCA Global G2 Root
11	Xinnet OV SSL	Signing Key	sha256RSA	2048 bits	CN = Xinnet OV SSL O = 北京新网数码信息技术有限公司 C = CN	4B78C0324A2442784E9F83F0D0FE336C7E0D934F	3C07D7EFC8D458F668C10D4F06F90503CCD25D59E2B3F1D58B32884D9E4E3809	UCA Global G2 Root
12	JoySSL DV Secure Server CA G1	Signing Key	sha384RSA	3072 bits	CN = JoySSL DV Secure Server CA G1 O = JoySSL Limited C = CN	2A56E8EF40E0A9999D6DD8129FB79B056B882DED	AA9CD0737407E9E9D9D86B145A2CFD7CD385C28BCF5996AA8D9A6DA5FC76F3A2	UCA Global G2 Root

#	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
13	JoySSL OV Secure Server CA G1	Signing Key	sha384RSA	3072 bits	CN = JoySSL OV Secure Server CA G1 O = JoySSL Limited C = CN	6BF2449C86D0C6DED85107661B2748792342CB95	0DD33FA366CA02808D29A5C1C456496AB5015C3604EB21C101406AF2533D998A	UCA Global G2 Root
14	KeepTrust DV TLS RSA CA G2	Signing Key	sha384RSA	3072 bits	CN = KeepTrust DV TLS RSA CA G2 O = Shanghai Huandu Info Tech Co. Ltd. C = CN	088B0DF30B0966297021D02C377300F5A7F4E7E9	352582CCC85B3944E3CD2505D9318F22ABEA418BFF29A0FE4D2C0DF280F200E3	UCA Global G2 Root
15	KeepTrust OV TLS RSA CA G2	Signing Key	sha384RSA	3072 bits	CN = KeepTrust OV TLS RSA CA G2 O = Shanghai Huandu Info Tech Co. Ltd. C = CN	F68D3850B96EA8BEFC50CA91247F1ABC9EA39D4D	CD50559A6DC5C704237EABF9A070B79F0CDFC1A79C3A6AC8C5E71E295A065D0A	UCA Global G2 Root
16	ZoTrus RSA DV SSL CA G1	Signing Key	sha384RSA	3072 bits	CN = ZoTrus RSA DV SSL CA G1 O = ZoTrus Technology Limited C = CN	EC1EBCB71E092769EFA715E89AA1677C33AA0F5A	E7EF1AD946214B32AF03CC287930D0464ED2C086D7A1447C6E27FC9217D4E16B	UCA Global G2 Root
17	ZoTrus RSA OV SSL CA G1	Signing Key	sha384RSA	3072 bits	CN = ZoTrus RSA OV SSL CA G1 O = ZoTrus Technology Limited C = CN	A0FA64A37EB83C7C194C51B7FE6A2BE8A39F78A4	3EC123D71DB27AE1DC8F877286C222F4167A2AE4FD7BCF370789EF4A9521B8	UCA Global G2 Root
18	JoySSL DV Secure Server CA	Signing Key	sha384RSA	3072 bits	CN = JoySSL DV Secure Server CA O = JoySSL Limited C = CN	807B3118B837D850FD1C4AD9879A5E426D00A1A4	AA9CD0737407E9E9D9D86B145A2CFD7CD385C28BCF5996AA8D9A6DA5FC76F3A2	UCA Global G2 Root
19	JoySSL OV Secure Server CA	Signing Key	sha384RSA	3072 bits	CN = JoySSL OV Secure Server CA O = JoySSL Limited C = CN	21507E5079E680B202C0FBC1AFAD8026DC52B8DD	0DD33FA366CA02808D29A5C1C456496AB5015C3604EB21C101406AF2533D998A	UCA Global G2 Root

#	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
20	KeepTrust DV TLS RSA CA G1	Signing Key	sha384RSA	3072 bits	CN = KeepTrust DV TLS RSA CA G1 O = Shanghai Huandu Info Tech Co. Ltd. C = CN	5063446A28FAC2B3D5122D01A63D9B85845026CC	A879CB01A2661C255B9C2B9BE0B20BA74EEA9546E21A82C570E177CF5BF4AEDA	UCA Global G2 Root
21	KeepTrust OV TLS RSA CA G1	Signing Key	sha384RSA	3072 bits	CN = KeepTrust OV TLS RSA CA G1 O = Shanghai Huandu Info Tech Co. Ltd. C = CN	04FA1B9DBC05CD575CC6518D5CDFE62CD151B0C8	FFD0D9EEEAAFBB4C44F71392F20A52E0F65896854933139640722DECFC2D4658	UCA Global G2 Root
22	ZoTrus RSA DV SSL CA	Signing Key	sha384RSA	3072 bits	CN = ZoTrus RSA DV SSL CA O = ZoTrus Technology Limited C = CN	7FEF9B0B9EB3F717A576BBC7580209DE731544B7	69C25861236502F0C223443FD851A2FB6ACB745BB814AD72BB2E50867C52C3BB	UCA Global G2 Root
23	ZoTrus RSA OV SSL CA	Signing Key	sha384RSA	3072 bits	CN = ZoTrus RSA OV SSL CA O = ZoTrus Technology Limited C = CN	E92D57AB2A4455799E257937123588FCDF187AC3	219C59CCD06D0210ADCF6E8125700D1578F69A0670A07FD9DDE99E4AC82524CD	UCA Global G2 Root
24	CT2 DV TLS RSA CA G1	Signing Key	sha384RSA	3072 bits	CN = CT2 DV TLS RSA CA G1 O = Tianyi Security Technology Co., Ltd. C = CN	8955C1DB0608F7A83C51CA3BF98F017B90098A73	4B316EDFC0780286571E430C0A94231B192B45666AF5DEBEE454FE08E4496383	UCA Global G2 Root
25	CT2 OV TLS RSA CA G1	Signing Key	sha384RSA	3072 bits	CN = CT2 OV TLS RSA CA G1 O = Tianyi Security Technology Co., Ltd. C = CN	27937BF574A8AF23A7F29E2B03CFACC7182B2EFA	A263B7CEFD1490D04FD0EC31D9695BAEE480EE861D12124C2BF8EBD8A893652F	UCA Global G2 Root
26	SHECA FREE DV TLS RSA CA G1	Signing Key	sha384RSA	3072 bits	CN = SHECA FREE DV TLS RSA CA G1 O = UniTrust C = CN	F18082839D6BB5C20A6A43C2D584A9F6F3EF2DC9	DFD9FB07A42E81216D6497FBC47BE53D829BBFD6A9188B02D5C8CDE29E01CF5C	UCA Global G2 Root

#	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
27	SHECA FREE DV TLS ECC CA G2	Signing Key	sha384RSA	384 bits	CN = SHECA FREE DV TLS ECC CA G2 O = UniTrust C = CN	84BCFE29594A85C0849FF0F21230812BE73F9BBC	81DB88F4CDE7345B0EC140E4A193720163DF9B787FABA0AF5A7EDACE6DC315A6	UCA Global G2 Root
28	SHECA DV TLS ECC CA G6	Signing Key	sha384RSA	384 bits	CN = SHECA DV TLS ECC CA G6 O = UniTrust C = CN	7E44A7C621F5F30E25293C07F288ECC82F7BD482	1F0570E418F9C89E094CB26EDA71B92BED81ACBB446B2300D398DDB739AB7A6C	UCA Global G2 Root
29	SHECA OV TLS ECC CA G6	Signing Key	sha384RSA	384 bits	CN = SHECA OV TLS ECC CA G6 O = UniTrust C = CN	2569CCEFDB564A83BAC15284500F13D86104FEE0	C4DA2C937523D42054FBB4AF694BB90FC7743C910EE048726241BD84C38509D9	UCA Global G2 Root
30	DNSPod DV TLS RSA CA G1	Signing Key	sha384RSA	3072 bits	CN = DNSPod DV TLS RSA CA G1 O = DNSPod, Inc. C = CN	4CF1C77BBB5F991923F8616FD712F9749C5AE55C	A07A7DEFCD1ED23F36D22AC33421F1D973583B12C96CA2496DE724C4494C0CD2	UCA Global G2 Root
31	DNSPod DV TLS ECC CA G1	Signing Key	sha384RSA	384 bits	CN = DNSPod DV TLS ECC CA G1 O = DNSPod, Inc. C = CN	B9A7EB6345ADB88940892F8B69930658DA9733CF	AACCD77057271FF5F605DF8CC5A44397E71CCE796EA79B8F1E8658FC9CD52464	UCA Global G2 Root
32	DNSPod OV TLS RSA CA G1	Signing Key	sha384RSA	3072 bits	CN = DNSPod OV TLS RSA CA G1 O = DNSPod, Inc. C = CN	38C22FB4856AB84A51911FE53A7FE2BE1103338F	F36592E33FD869E917E33BADE683A4EC20809D5C8B493A1427BA6DC066CB5AE3	UCA Global G2 Root
33	DNSPod OV TLS ECC CA G1	Signing Key	sha384RSA	384 bits	CN = DNSPod OV TLS ECC CA G1 O = DNSPod, Inc. C = CN	586EA65733443DCE3CED5DEBF47E000F0E81B28D	8C4BFF9AE3F079E50208F84E4DA658AB441109686861FFCEE50D4A8662C2EEA1	UCA Global G2 Root
34	Keymatic Secure Domain RSA CA G1	Signing Key	sha384RSA	3072 bits	CN = Keymatic Secure Domain RSA CA G1 O = PKI(Chongqing) Limited C = CN	8ED096D6E8A4D935F386EBDA0B592E40521B0CBB	F3C9431A163BECE79562093F0734DF6ED05618551CFEE0ABA949A77E959D8AAE	UCA Global G2 Root

#	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
35	Keymatic Secure Domain ECC CA G1	Signing Key	sha384RSA	384 bits	CN = Keymatic Secure Domain ECC CA G1 O = PKI(Chongqing) Limited C = CN	C1286B590B198916D776E6661E57D4460812EDDF	B07D2ACA4F29E2449B5ADB7CCB31C64C43854044A2DAA2AC838788026C684C0C	UCA Global G2 Root
36	Keymatic Secure Business RSA CA G1	Signing Key	sha384RSA	3072 bits	CN = Keymatic Secure Business RSA CA G1 O = PKI(Chongqing) Limited C = CN	5693F449C7E448C3C3D2BE86397E33368163A377	5523644185E21EF943A505A1C438167DA1FE7B14BEF2D243E53DE8C2B4263EB7	UCA Global G2 Root
37	Keymatic Secure Business ECC CA G1	Signing Key	sha384RSA	384 bits	CN = Keymatic Secure Business ECC CA G1 O = PKI(Chongqing) Limited C = CN	23368DE013A9BB36D76A66E1128EDA5F4A3620D5	75C4AF6628E7D01DD369593EFD727E3560ED9DDD67B04325655821BD23281A2B	UCA Global G2 Root
38	sslTrus RSA DV TLS CA G2	Signing Key	sha384RSA	3072 bits	CN = sslTrus RSA DV TLS CA G2 O = sslTrus C = CN	DEE386BAC52E630164E0C142943C3202967C6891	B3A5BED750BCE5A08C75E0012B0A6A67954952BC8D12520514CC15CBB0B17039	UCA Global G2 Root
39	sslTrus ECC DV TLS CA G2	Signing Key	sha384RSA	384 bits	CN = sslTrus ECC DV TLS CA G2 O = sslTrus C = CN	624679EBA47FFA4CD98D6FFFDE6D6F7FE49E86E9	32CAA961415106CF471CEA5B15C66464A907C99861A297C359D174624BADB92F	UCA Global G2 Root
40	sslTrus RSA OV TLS CA G2	Signing Key	sha384RSA	3072 bits	CN = sslTrus RSA OV TLS CA G2 O = sslTrus C = CN	0EDFB68948064E10818E3C8108C824BB8B308F62	F0E647B5A2869A3487507A90549AF039896DB8B0F0E7CF92EF3AB567F3EC5E5C	UCA Global G2 Root
41	sslTrus ECC OV TLS CA G2	Signing Key	sha384RSA	384 bits	CN = sslTrus ECC OV TLS CA G2 O = sslTrus C = CN	BEE114C1BEF84DA5E3D4E41FCA0D1F81A90C0FE0	06B7E611243D2901B964FF6D0C53A2DB52BA2E1D41E17D74950E16605D9A2C90	UCA Global G2 Root

#	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
42	HTTPS Automation Research RSA DV SSL CA G1	Signing Key	sha384RSA	3072 bits	CN = HTTPS Automation Research RSA DV SSL CA G1 O = Shenzhen Yamu Security Technology Co., Ltd. C = CN	0FB6A84D71E5B1B38F9E72D6BBC06A147FE4D03B	1E426FF0F51EB4C285788B4418D2DAB21097230CED81119BA178A20AB1AABF67	UCA Global G2 Root
43	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	C1AFC65B1E813B0E6146E6AA5341681272ABE9A38D59F7BD1B27B729834A0D9C	Certum Trusted Network CA
44	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	3DD69C5BE170F943F804D1D31FE8F916C0C0226CDDD7AEA9AA9A0CDFD3474361	Certum Trusted Network CA
45	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	BB61408AED9F530B2EC0545E53BA2C8EBEAA57D9976447DB1663CED4600CD6B7	Certum Trusted Network CA
46	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	BFA95C5DF164B659FA32F6D10564D7170DDE661A853A782E6AB63639433BCB41	Certum Trusted Network CA
47	UCA Extended Validation Root	Root Key	sha256RSA	4096 bits	CN = UCA Extended Validation Root O = UniTrust C = CN	D9743AE4303D0DF712DC7E5A059F1E349AF7E114	D43AF9B35473755C9684FC06D7D8CB70EE5C28E773FB294EB41EE71722924D24	UCA Extended Validation Root
48	SHECA RSA Extended Validation Server CA	Signing Key	sha256RSA	2048 bits	CN = SHECA RSA Extended Validation Server CA O = UniTrust C = CN	3B4B252A77372AFCB97FEDA8BDAF2299FC5DC5F4	4FD6FA527157EEA463689D7A4C2B934EF222279725413893D9847242C85CA9DF	UCA Extended Validation Root

#	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
49	SHECA EV Server CA G3	Signing Key	sha256RSA	2048 bits	CN = SHECA EV Server CA G3 O = UniTrust C = CN	54E972FB78669FE5CBF33B8F98465553739C0B84	7EF3F89456CE636557B20C5DFB37F98C253A0B660D2E9E5E7845CAF9C038C7C1	UCA Extended Validation Root
50	SHECA OV Server CA G6	Signing Key	sha256RSA	2048 bits	CN = SHECA OV Server CA G6 O = UniTrust C = CN	FB7DCE4905B420BCFFBF0D8471ADAE0135F961A0	264DF1458FB5EF1FC9DF9F1345E84A6CC1A471CF475AE7598FF52B86713519FB	UCA Extended Validation Root
51	SHECA OV Server CA G7	Signing Key	sha256RSA	2048 bits	CN = SHECA OV Server CA G7 O = UniTrust C = CN	A0F344BA17512C7776AB4442C5534B16AB5F0DAA	F6F8BCD413C9733166E85843B468DD36E727152D9A37B15129C0E7648ECEE639	UCA Extended Validation Root
52	SHECA Extended Validation SSL CA	Signing Key	sha256RSA	2048 bits	CN = SHECA Extended Validation SSL CA O = UniTrust C = CN	4D140DEA6B559C0CA6E1BB7BE86A966D175E7CB5	25BFDB1C5FE2CCE051EC6DFBF2BB24E78C92F969B1BB37867DAEDF93D1A7AE7E	UCA Extended Validation Root
53	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
54	SHECA DV Server CA 1A	Signing Key	sha384RSA	4096 bits	CN = SHECA DV Server CA 1A O = UniTrust C = CN	653740E0BBF43905206A8C9CA0ACB3BBD6968CA0	D3D4A040BB41A695A96E3AAD93814CF7EF219D5819206E947B44DCC5B8E5E272	UniTrust Global Root CA R1
55	SHECA OV Server CA 1A	Signing Key	sha384RSA	4096 bits	CN = SHECA OV Server CA 1A O = UniTrust C = CN	8CD02E82008EE2DEFF71F61A105C74A826E858D1	9A3DB0F0FB0FF4F974A4E0C510A7C13D350485B1E6CDF5A899BB24D0F499E9BD	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
56	SHECA EV Server CA 1A	Signing Key	sha384RSA	4096 bits	CN = SHECA EV Server CA 1A O = UniTrust C = CN	73E36DF62D862F57DF69A53687231C85E0170216	2F1CA1A5C0D7AE58C7ADFC69D4C57EE815F39C0F3D1F982E3AC76D25AB723995	UniTrust Global Root CA R1
57	UniTrust Global Root CA R2	Root Key	sha384ECDSA	384 bits	CN = UniTrust Global Root CA R2 O = UniTrust C = CN	E45366B7B7A4E9D7CCC121E04ACFCCAC01BC72BC	78919B35D1C615595A51328A5C546083B4D5320724A258695B991F2F61C4DCC7	UniTrust Global Root CA R2
58	SHECA DV Server CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA DV Server CA 2A O = UniTrust C = CN	A1221170BEC8665F6ECB104C4EDB38EA9C1F914D	69201DC24E4127FFA5B41A0DDF0A1A005C00F334B003F1008924CBF998E1827C	UniTrust Global Root CA R2
59	SHECA OV Server CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA OV Server CA 2A O = UniTrust C = CN	98CDEC338767F39422373810B735BA7C683A8259	8E2CA2825C2039804A7A1CC54B002EA1DB30AC489698F039527BF1602132F611	UniTrust Global Root CA R2
60	SHECA EV Server CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA EV Server CA 2A O = UniTrust C = CN	44661C71EF69B7930AB5B771D83B114CFA843D77	93E49170D20F54DA701118A5ABDCDDA4FFCF334CDB2D8D80599AB62848C85F80	UniTrust Global Root CA R2
61	UniTrust Global TLS ECC Root CA R2	Root Key	sha384ECDSA	384 bits	CN = UniTrust Global TLS ECC Root CA R2 O = UniTrust C = CN	7935AD798A95305C3E05A675161A97000F6FCC90	6C689FC6B014A1FB0CDEB5A3996171C15E7286106028532E0210CEA8D9CD4E97	UniTrust Global TLS ECC Root CA R2
62	SHECA DV TLS ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA DV TLS ECC CA 2A O = UniTrust C = CN	CB65E62F50175F2C172B433F3A043CD213569A66	D690D8722EA89CD7617901449520653339386AC4939F7EC5C1B195D9C3C95FA4	UniTrust Global TLS ECC Root CA R2

#	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
63	SHECA EV TLS ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA EV TLS ECC CA 2A O = UniTrust C = CN	B353900B5E40A4952EA85A27F413ABBAD631F233	05E4C4B1F258030690E6793C9C13C6F6AE234F68E5C41236FDC919B7F589032F	UniTrust Global TLS ECC Root CA R2
64	SHECA OV TLS ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA OV TLS ECC CA 2A O = UniTrust C = CN	A065578C43B2546C4E18DF86AED56725A9B7659C	08BA64405A3406C97BDCBD0E44224E6DD341F3EC93F1368457DFA7CAC88BE150	UniTrust Global TLS ECC Root CA R2
65	UniTrust Global TLS RSA Root CA R1	Root Key	sha384RSA	4096 bits	CN = UniTrust Global TLS RSA Root CA R1 O = UniTrust C = CN	F2ADBFAB6708F09672E633D65175A24759C900C4	4BABE0E9328D5DAE17936F3DDAA2442BFBDD0873F92FB8D1FBBD3D9894649AD9	UniTrust Global TLS RSA Root CA R1
66	SHECA DV TLS RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA DV TLS RSA CA 1A O = UniTrust C = CN	C5E3A87F7EEDBC3E7108B34EF490EF2F2F1367D1	FFABEA74895DC0C78C224597472CF6937E0D740EF49DC2256C8E75A2A2A15EDE	UniTrust Global TLS RSA Root CA R1
67	SHECA EV TLS RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA EV TLS RSA CA 1A O = UniTrust C = CN	60651A135EAB2B98A5A1041B3057A1D02FC612E5	B2525A5966CA68CA7F504F0A21FD73847D174F89B48852A3E970588E1EAFC774	UniTrust Global TLS RSA Root CA R1
68	SHECA OV TLS RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA OV TLS RSA CA 1A O = UniTrust C = CN	F463091C1E2788B75DBBE91644B1744A34F34B46	7F8EF707C2D9A4B7D4ED5FDDC8AF4A64D99BF297D03F8F01C4375DE74B1C7DE1	UniTrust Global TLS RSA Root CA R1