pwc 羅兵咸永道

Independent practitioner's assurance report

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

Scope

We have been engaged to perform a reasonable assurance engagement on the accompanying management's assertion of SHECA for its Certification Authority (CA) operations at Shanghai (including Facility 1 and Facility 2), China for the period from April 1, 2023 to March 31, 2024 for its CAs as enumerated in Attachment A, SHECA has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environment control practices in its:
  - UniTrust Certification Practice Statement v3.7.7;
  - UniTrust Certification Practice Statement v3.7.6;
  - UniTrust Certification Practice Statement v3.7.5;
  - UniTrust Certification Practice Statement v3.7.4;
  - UniTrust Certification Practice Statement v3.7.3;
  - UniTrust Certification Practice Statement v3.7.2;
  - UniTrust Certificate Policy v1.5.5;
  - UniTrust Certificate Policy v1.5.4;
  - UniTrust Certificate Policy v1.5.3;
  - UniTrust Certificate Policy v1.5.2;
  - UniTrust Certificate Policy v1.5.1;
  - UniTrust Certificate Policy v1.5.0;
  - UniTrust Event Certification Policy & Certification Practice Statement v1.7;
  - UniTrust Event Certification Policy & Certification Practice Statement v1.6; and
  - UniTrust Event Certification Policy & Certification Practice Statement v1.5,

- maintained effective controls to provide reasonable assurance that:
  - SHECA's Certification Practice Statements are consistent with its Certificate Policies; and
  - SHECA provides its services in accordance with its Certificate Policies and 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 v2.2.2.

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.

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

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 v2.2.2.

Our Independence and Quality Management

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

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

Practitioner's Responsibilities

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

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

A reasonable assurance engagement involves performing procedures to obtain sufficient appropriate evidence whether the management's assertion of SHECA is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.2.2. 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 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.

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

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

Inherent Limitation

Because of the nature and inherent limitations of controls, SHECA's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorised access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any opinion based on our findings to future periods is subject to the risk that changes may alter the validity of such opinion.

Opinion

In our opinion, the management's assertion of SHECA, for the period from April 1, 2023 to March 31, 2024, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.2.2.

Emphasis of Matter

Without modifying our opinion, we draw attention to the fact that this report does not include any representation as to the quality of SHECA's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities v2.2.2, nor the suitability of any of SHECA's services for any customer's intended purpose.

Other Matter

The UniTrust Global Root CA R1 (Attachment A #48), UniTrust Global Root CA R2 (Attachment A #55), UniTrust Global Root CA R3 (Attachment A #59) CAs did not issue certificates during the period April 1, 2023 to March 31, 2024 and were maintained online to provide revocation status information only.

SHECA's management has disclosed 12 incidents (see Attachment B) during the period from April 1, 2023 to March 31, 2024. The remedial actions and the root causes of these incidents undertaken by SHECA have been posted publicly in the online forums of the

Bugzilla site, as well as the online forums of individual internet browsers that comprise the CA/Browser Forum.

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 Auth orities v2.2.2 designed for this purpose. As a result, the management's assertion of SHECA may not be suitable for another purpose. This report is intended solely for the management of SHECA in connection with obtaining and displaying the WebTrust Seal on its website after submitting the report to the related authority in connection with the WebTrust Principles and Criteria for Certification Authorities v2.2.2.

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

Use of the WebTrust seal

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

PricewaterhouseCoopers
Certified Public Accountants

Hong Kong, 24 May 2024

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

pwc

羅兵咸永道

Attachment A

The list of keys and certificates in scope for the period from April 1, 2023 to March 31, 2024 is as follow:

#	Key Name	Key Type	Signature Algorithm	Key Size	Subject DN	Subject Key Identifier	Certificates Thumbprint (SHA256)	Certificate Signed by
1	UCA Root G2	Root Key	sha256RSA	2048 bits	CN = UCA Root G2 O = UniTrust C = CN	E4BB2C9FB2B51C8831AF7FCBDCF4052BE085F701	A07919A6391BCD6E15FB33A41B43A938EF3D19CF54F0198EC29D02364BC5A0EC	UCA Root G2
2	SHECA G2	Signing Key	sha256RSA	2048 bits	CN = SHECA G2 O = UniTrust C = CN	5688DEE3184382B772A426EB44A962D087C4AC26	69275DE8AF892E26E1B5339A664C194550799372F13CA6FB4966408F6A43C5B4	UCA Root G2
3	SHECA G2	Signing Key	sha256RSA	2048 bits	CN = SHECA G2 O = UniTrust C = CN	5688DEE3184382B772A426EB44A962D087C4AC26	23434A3078ADBE51DF267504F5655107ED1AA4E555D3DF21F479F1B4E4610A08	UCA Root G2
4	GlobalSign China CA for AATL	Signing Key	sha256RSA	2048 bits	CN = GlobalSign China CA for AATL O = GlobalSign China L = Shanghai S = Shanghai C = CN	FCAD8AADBF323AFF97C09BD74A7039888919D46A	D883436D97B08B008810D2EF3852D322E1D3528C751D3B23FF0C80803ED1CFAE	UCA Root G2
5	UCA Root SM2	Root Key	SM2	256 bits	CN = UCA Root SM2 O = UniTrust C = CN	EEE8B09CD5DCEC73FDEF7CFA502CC6C140E64CB3	307C77562B1532AE5FA6E63ED597CD54A0CBCC111F3598A7CCB2E19DD1351362	UCA Root SM2
6	UniTrust DV Secure Server CA G4	Signing Key	SM2	256 bits	CN = UniTrust DV Secure Server CA G4 O = UniTrust C = CN	ADA611696054F898CED269542A29DF239484E833	68B5E5FCA21925C5AF6628341FE6DBD187C6E66AEEF5F58295DCD7238FF56AD8	UCA Root SM2
7	UniTrust OV Secure Server CA G4	Signing Key	SM2	256 bits	CN = UniTrust OV Secure Server CA G4 O = UniTrust C = CN	D6546FA6587275420BF204794C4C6DE4368A8BD5	E75A9D14B5C5FF14779F0DC8A7889EE757788DC82706D95B4E2AF039098FA72C	UCA Root SM2
8	SHECA SM2	Signing Key	SM2	256 bits	CN = SHECA SM2 O = UniTrust C = CN	893104917B43AAAA9ABF841D9B86EEF0B87099A0	F5F6192276AED2141B3A66FD66724D46C5A58CACF618CAA5B5AA546ED5865207	UCA Root SM2

pwc

羅兵咸永道

#	Key Name	Key Type	Signature Algorithm	Key Size	Subject DN	Subject Key Identifier	Certificates Thumbprint (SHA256)	Certificate Signed by
9	TrustAsia SM2 DV TLS CA - S1	Signing Key	SM2	256 bits	CN = TrustAsia SM2 DV TLS CA - S1 O = TrustAsia Technologies, Inc. C = CN	1B40CF756BB3E9D42B6AE0CCA449D5A26FE48F2A	FB812E1561383E0020103977D7E64D18B3587BC092F9DEC67600DE2A8493352C	UCA Root SM2
10	TrustAsia SM2 OV TLS CA - S1	Signing Key	SM2	256 bits	CN = TrustAsia SM2 OV TLS CA - S1 O = TrustAsia Technologies, Inc. C = CN	3623100989022D63A4C9E816BC531490AA2A01F7	2DBE68A196611EC658022F62607FBC0AA2000FD3147028EB2B16355B6D296EDF	UCA Root SM2
11	TrustAsia SM2 Identity CA - S1	Signing Key	SM2	256 bits	CN = TrustAsia SM2 Identity CA - S1 O = TrustAsia Technologies, Inc. C = CN	73075D5EFBF48320ED005F013AD1930E3FF432F2	BACE521585871388E4B3ECF44B5B4A965CCFD995C72D8813B61E643C77F1298D	UCA Root SM2
12	SHECA SM2 Identity CA G1	Signing Key	SM2	256 bits	CN = SHECA SM2 Identity CA G1 O = UniTrust C = CN	687C2F9B2E68A2DFCE11115411A6B60E6CEE2520	490BA44A5C4061D487EF1C945EC4889770A1F31299F0083045192D8978C25D7E	UCA Root SM2
13	CECloud Secure Server CA V1	Signing Key	SM2	256 bits	CN = CECloud Secure Server CA V1 O = 中国电子系统技术有限公司 C = CN	3D017054EBD1DAE2FA72558A7B4AD4112EC2789C	D973269DE727110F2577F12FC7039F204C8688F90479A60A6D918181E96BC921	UCA Root SM2
14	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	9BEA11C976FE014764C1BE56A6F914B5A560317ABD9988393382E5161AA0493C	UCA Global G2 Root
15	SHECA SMIME CA G1	Signing Key	sha256RSA	2048 bits	CN = SHECA SMIME CA G1 O = UniTrust C = CN	1FA80B4DCF9CA6A53ADAB096AB9957B90A9B7F5D	8100D384D6C4529883C37C37C68FD4903C41CCBCB9033A9C733A6AF0806E1DE7	UCA Global G2 Root
16	SHECA RSA Code Signing CA G3	Signing Key	sha256RSA	2048 bits	CN = SHECA RSA Code Signing CA G3 O = UniTrust C = CN	FD7EC87AC2771C5687D2AEF807C7426A1B7C42A8	C7E976AA77E92491C269840B2F1461E65147A2BB181EE59AB63BCD86704FE456	UCA Global G2 Root

#	Key Name	Key Type	Signature Algorithm	Key Size	Subject DN	Subject Key Identifier	Certificates Thumbprint (SHA256)	Certificate Signed by
17	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
18	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
19	SHECA RSA Time Stamp Authority G1	Signing Key	sha256RSA	2048 bits	CN = SHECA RSA Time Stamp Authority G1 O = UniTrust C = CN	6FC5770C4E825E4B544B30BD9933F408571A3DB4	86EE4A2F93137CA8887674078B394070F189B3049DD2D24053AE92924254C668	UCA Global G2 Root
20	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
21	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
22	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
23	SHECA Code Signing CA G4	Signing Key	sha256RSA	3072 bits	CN = SHECA Code Signing CA G4 O = UniTrust C = CN	73C3B39021CBF23BDA23D351F295C58BC678EE47	8F0C3E06A16E3EA7C9B15A848076ED15E51DA0B6F1AFA274EDE2B9102191FE0F	UCA Global G2 Root
24	SHECA Time Stamping CA G2	Signing Key	sha256RSA	3072 bits	CN = SHECA Time Stamping CA G2 O = UniTrust C = CN	CFDD9E670A6CB17E2C1A4F595387B2369BF96994	422C71F8DB9FDA2C65458B52363DB6FDC4E37B436774BCF97518F3F42EC725F1	UCA Global G2 Root
25	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

pwc

羅兵咸永道

#	Key Name	Key Type	Signature Algorithm	Key Size	Subject DN	Subject Key Identifier	Certificates Thumbprint (SHA256)	Certificate Signed by
26	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
27	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
28	SHECA Global G3 Code Signing	Signing Key	sha256RSA	2048 bits	CN = SHECA Global G3 Code Signing O = UniTrust S = Shanghai C = CN	F73DF939A8D98754AC778EF5D995EEF835AB9439	EAA5AD8E9A2FA992354B2FF4254BEB08A632F7F17602604DDED58D73D616D844	UCA Global G2 Root
29	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
30	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
31	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	C1AFC65B1E813B0E6146E6AA5341681272ABE9A38D59F7BD1B27B729834A0D9C	Certum Trusted Network CA
32	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	3DD69C5BE170F943F804D1D31FE8F916C0C0226CDDD7AEA9AA9A0CDFD3474361	Certum Trusted Network CA
33	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	BB61408AED9F530B2EC0545E53BA2C8EBEAA57D9976447DB1663CED4600CD6B7	Certum Trusted Network CA

pwc

羅兵咸永道

#	Key Name	Key Type	Signature Algorithm	Key Size	Subject DN	Subject Key Identifier	Certificates Thumbprint (SHA256)	Certificate Signed by
34	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	BFA95C5DF164B659FA32F6D10564D7170DDE661A853A782E6AB63639433BCB41	Certum Trusted Network CA
35	UCA Extended Validation Root	Root Key	sha256RSA	4096 bits	CN = UCA Extended Validation Root O = UniTrust C = CN	D9743AE4303D0DF712DC7E5A059F1E349AF7E114	D43AF9B35473755C9684FC06D7D8CB70EE5C28E773FB294EB41EE71722924D24	UCA Extended Validation Root
36	SHECA RSA Extended Validation Code Signing CA	Signing Key	sha256RSA	2048 bits	CN = SHECA RSA Extended Validation Code Signing CA O = UniTrust C = CN	8E40665F6AA940C2B9F1F04A22639564593707E5	D404FAFA4BA2F426B66CD219C6DA84F91C0FB7CB58429EC8077E2A764314D55D	UCA Extended Validation Root
37	SHECA RSA Extended Validation Server CA	Signing Key	sha256RSA	2048 bits	CN = SHECA RSA Extended Validation Server CA O = UniTrust C = CN	3B4B252A77372AFCB97FEDA8BDAF2299FC5DC5F4	4FD6FA527157EEA463689D7A4C2B934EF2222797254138 93D9847242C85CA9DF	UCA Extended Validation Root
38	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
39	SHECA EV Code Signing CA G2	Signing Key	sha256RSA	3072 bits	CN = SHECA EV Code Signing CA G2 O = UniTrust C = CN	5007CC4DF6F4BA37FC13CE1F2D22C956D89EA503	DD84169585A2E7A216AECD4083265A8EB51A64F7C6F1943671F8584C73F79A74	UCA Extended Validation Root
40	SHECA OV Server CA G6	Signing Key	sha256RSA	2048 bits	CN = SHECA OV Server CA G6 O = UniTrust C = CN	FB7DCE4905B420BCFFBF0D8471ADAE0135F961A0	264DF1458FB5EF1FC9DF9F1345E84A6CC1A471CF475AE7598FF52B867135 19FB	UCA Extended Validation Root
41	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
42	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

pwc

羅兵咸永道

#	Key Name	Key Type	Signature Algorithm	Key Size	Subject DN	Subject Key Identifier	Certificates Thumbprint (SHA256)	Certificate Signed by
43	SHECA Extended Validation Code Signing CA	Signing Key	sha256RSA	2048 bits	CN = SHECA Extended Validation Code Signing CA O = UniTrust C = CN	7498996F6A15C0062520851CAF2B316B87EDA3DB	A392C645B9A5AD6A214F19DE776346BC7DD6BB15818E433886DAC54EE6661852	UCA Extended Validation Root
44	UniTrust Event Certificate Root CA R1	Root Key	sha384RSA	4096 bits	CN = UniTrust Event Certificate Root CA R1 O = UniTrust C = CN	D7418BEED45FC6E97D69108608AC7EE48BA0727E	3200B1BC5CF8F8BC0A382BD7809166A221600747DEC386D2625959CD75A28212	UniTrust Event Certificate Root CA R1
45	SHECA Event Certificate CA G1	Signing Key	sha256RSA	2048 bits	CN = SHECA Event Certificate CA G1 O = UniTrust C = CN	2A4D7575347FFFB46A57513816FFA99EEAAF0F4F	32AE6837AEF2DABBC8C19385A57A19FC97F6BDB8384B1ADCCDEAED3A891A3A0F	UniTrust Event Certificate Root CA R1
46	Orient Fortune Securities Co., Ltd Identity CA G1	Signing Key	sha256RSA	2048 bits	CN = Orient Fortune Securities Co., Ltd Identity CA G1 O = 东方财富证券股份有限公司 C = CN	8F155742AFDF87B618F8622DAB2E07091A796249	115250822139D3C6A49C821ABB19630FAC617190DAA3CF7373D3C95F082CBDF7	UniTrust Event Certificate Root CA R1
47	Shanghai Eastmoney Futures Co., Ltd. Identity CA G1	Signing Key	sha256RSA	2048 bits	CN = Shanghai Eastmoney Futures Co., Ltd Identity CA G1 O = 上海东方财富期货有限公司 C = CN	D09AE4CC4499268F8D72F83789C45F3F11B7BA8D	B4800869058B4B74CA970B3414FEDE2F676D90F979E4961325AD72B13ABE8866	UniTrust Event Certificate Root CA R1
48	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
49	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

pwc

羅兵咸永道

#	Key Name	Key Type	Signature Algorithm	Key Size	Subject DN	Subject Key Identifier	Certificates Thumbprint (SHA256)	Certificate Signed by
50	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
51	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
52	SHECA Code Signing CA 1A	Signing Key	sha384RSA	4096 bits	CN = SHECA Code Signing CA 1A O = UniTrust C = CN	21B34B4FC6DD33246E861BACEBF182D7EFCA2CDA	59E3EF6680BCC0B1162DED4929D37E698C6A5CBEE075C03F1173AD653CF91CED	UniTrust Global Root CA R1
53	SHECA EV Code Signing CA 1A	Signing Key	sha384RSA	4096 bits	CN = SHECA EV Code Signing CA 1A O = UniTrust C = CN	510BE3C14EABDFEA38FF434E2C97339C0BFC27A9	03E04A3C2B5200BB27C679A37261852BAC7D46F3F371E4ECA80225AE288E4CFC	UniTrust Global Root CA R1
54	SHECA Time Stamping CA 1A	Signing Key	sha384RSA	4096 bits	CN = SHECA Time Stamping CA 1A O = UniTrust C = CN	8FBFB44A46F647EDF6EB8A0B5E1609430896FA46	2DFDBF6CEC0587B55F1300F109BC46EFD16BC7EB5F43CAE563953D87C7B432C4	UniTrust Global Root CA R1
55	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
56	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
57	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
58	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
59	UniTrust Global Root CA R3	Root Key	SM2	256 bits	CN = UniTrust Global Root CA R3 O = UniTrust C = CN	3B15E62B1C9F5015B64EA16D163A558AF4905FB5	6A19BCC7FAD2A5664F779BF143A72A2B079AC476E56FACBA48C352635CB4718F	UniTrust Global Root CA R3

pwc

羅兵咸永道

#	Key Name	Key Type	Signature Algorithm	Key Size	Subject DN	Subject Key Identifier	Certificates Thumbprint (SHA256)	Certificate Signed by
60	SHECA DV Server CA 3A	Signing Key	SM2	256 bits	CN = SHECA DV Server CA 3A O = UniTrust C = CN	26924A66CDEDA9AD2DD7D0AE53C5DE95436A2C61	E464F2E140327DA8326C53A2FBA322F183E6DEFC56888A0811195265650BCAD1	UniTrust Global Root CA R3
61	SHECA OV Server CA 3A	Signing Key	SM2	256 bits	CN = SHECA OV Server CA 3A O = UniTrust C = CN	6F465A89CFB174BB558EB3A56D08093233E36D2F	19B057AB0827E37C8EB2EA7C04292068A253A3BEDC0C45848881C0BA78E717CF	UniTrust Global Root CA R3
62	SHECA EV Server CA 3A	Signing Key	SM2	256 bits	CN = SHECA EV Server CA 3A O = UniTrust C = CN	988B07A078C97576AF0CA1A723E87F4E9B482689	7F4A5FBCA47F8904D0AEA5D3BFA5759C4768BA6510EB1FEB5E5B076D12907741	UniTrust Global Root CA R3
63	UniTrust Global Code Signing ECC Root CA R2	Root Key	sha384ECDSA	384 bits	CN = UniTrust Global Code Signing ECC Root CA R2 O = UniTrust C = CN	D6E2F5C7B440515C5A3A5C490EFCB8C239503CDB	8854E81F9C6B47E438BBAE17E41F8BE4E68589AFD31A48BEE3F203F6DD3DA517	UniTrust Global Code Signing ECC Root CA R2
64	SHECA Code Signing ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA Code Signing ECC CA 2A O = UniTrust C = CN	3A5576122E385EB715671EE385BF1E3D0AC77A1A	953707AE07AF34970462E8C02AC3D10949D3684D063385277F31869508007D23	UniTrust Global Code Signing ECC Root CA R2
65	SHECA EV Code Signing ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA EV Code Signing ECC CA 2A O = UniTrust C = CN	BFAE7906E9776B61D01E4579986F2698B66DF25E	545BD126658352B306EE74185173F1774A79467A26E9BB6AE0ED44D86615DE5A	UniTrust Global Code Signing ECC Root CA R2
66	UniTrust Global Code Signing RSA Root CA R1	Root Key	sha384RSA	4096 bits	CN = UniTrust Global Code Signing RSA Root CA R1 O = UniTrust C = CN	60C14C87BDAAB27B678E4EA7921C519B481BA860	6357353A4BBCA3D5A158C95BE9DC90F0B3E2F6A6310FD5371FCB4C41E5E1BB4C	UniTrust Global Code Signing RSA Root CA R1
67	UniTrust Global SMIME ECC Root CA R2	Root Key	sha384ECDSA	384 bits	CN = UniTrust Global SMIME ECC Root CA R2 O = UniTrust C = CN	2D4D94407CFFC45D4357F190557448CF6CBEA343	6F4E2464D216A1E0B558BB204259B4A545AEB948957AA3EAF11B2F4DE1AFEF10	UniTrust Global SMIME ECC Root CA R2
68	SHECA IV SMIME ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA IV SMIME ECC CA 2A O = UniTrust C = CN	EBC1D6F67F2909A9928A90B4295818A02F3CAF1B	E82D794C1AC79F9BEBF3B6D98A237F84C15FD40C3ABB86C2214E699414F8FF54	UniTrust Global SMIME ECC Root CA R2

pwc

羅兵咸永道

#	Key Name	Key Type	Signature Algorithm	Key Size	Subject DN	Subject Key Identifier	Certificates Thumbprint (SHA256)	Certificate Signed by
69	SHECA MV SMIME ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA MV SMIME ECC CA 2A O = UniTrust C = CN	FE0328035B693E5EDC5FAE0B742735DCC38C66F0	D7C4AB9D315AE8B889DA902C55264295D8CDC0F5471370490F4D4585E2C3C6D3	UniTrust Global SMIME ECC Root CA R2
70	SHECA OV SMIME ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA OV SMIME ECC CA 2A O = UniTrust C = CN	BD34144476B06D0F264C3CA9C349AC7153D4EF55	229B7FBCA2361DE63171067DE91DFFB3D2FA71A5ABE51CA41D5300C5750D2F0E	UniTrust Global SMIME ECC Root CA R2
71	UniTrust Global SMIME RSA Root CA R1	Root Key	sha384RSA	4096 bits	CN = UniTrust Global SMIME RSA Root CA R1 O = UniTrust C = CN	DF08E3E977C1F0FBF5F8D419504C7719F206CBA3	F0F255ADA2A643C0A1E7C8F54F3ED3DD25EF0E7378E76F7C127517ECFD952803	UniTrust Global SMIME RSA Root CA R1
72	SHECA IV SMIME RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA IV SMIME RSA CA 1A O = UniTrust C = CN	D38BCDC445B1E8D0AFDD8BE8E4A6B5B30A71EF4E	82BA6F1067468383757DF53F1628258043BBB972E1CAD31FD7AAD0ADD66A5B53	UniTrust Global SMIME RSA Root CA R1
73	SHECA MV SMIME RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA MV SMIME RSA CA 1A O = UniTrust C = CN	5A4AEFED9AE84052DA320BBB32C4E529ECDC5255	92148A115D26B287254B36164164B2220EE36B405D3B708CF5B7AB060C66B1FE	UniTrust Global SMIME RSA Root CA R1
74	SHECA OV SMIME RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA OV SMIME RSA CA 1A O = UniTrust C = CN	C061C3D053C9F412C5C9192DBB638305E4CA7EF8	6B661B964F2359C4CA68355243A2EEEDA9BACDA191D103A0C1119EC892018AC7	UniTrust Global SMIME RSA Root CA R1
75	UniTrust Global Time Stamping ECC Root CA R2	Root Key	sha384ECDSA	384 bits	CN = UniTrust Global Time Stamping ECC Root CA R2 O = UniTrust C = CN	C20E70D5E4015590A717B62DDDB5389D7627A1B7	90711D905CFF3C773A7320B5188A960C8A7D9E5966FA73284D64A4BF3E2FDA48	UniTrust Global Time Stamping ECC Root CA R2
76	SHECA Time Stamping ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA Time Stamping ECC CA 2A O = UniTrust C = CN	41315BE8FD8C3C65630168307A0B30EC097F1069	0E3FC096DDCC3205047F9042D57882A1144107243C47CDE6FFFDE403A5B7CA04	UniTrust Global Time Stamping ECC Root CA R2
77	UniTrust Global Time Stamping RSA Root CA R1	Root Key	sha384RSA	4096 bits	CN = UniTrust Global Time Stamping RSA Root CA R1 O = UniTrust C = CN	DA891E9DC30F38DAB0896CCDC5FDD7504F155B30	1759727D9E6679B069DD3AFA910E2779C42007AAB206A169C66E6E2A3D1774B0	UniTrust Global Time Stamping RSA Root CA R1

pwc

羅兵咸永道

#	Key Name	Key Type	Signature Algorithm	Key Size	Subject DN	Subject Key Identifier	Certificates Thumbprint (SHA256)	Certificate Signed by
78	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	6C689FC6B014A1FB0CDEB5A3996171C15E728610602853 2E0210CEA8D9CD4E97	UniTrust Global TLS ECC Root CA R2
79	SHECA DV TLS ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA DV TLS ECC CA 2A O = UniTrust C = CN	CB65E62F50175F2C172B433F3A043CD213569A66	D690D8722EA89CD761790144952065 3339386AC4939F7EC5C1B195D9C3C95FA4	UniTrust Global TLS ECC Root CA R2
80	SHECA EV TLS ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA EV TLS ECC CA 2A O = UniTrust C = CN	B353900B5E40A4952EA85A27F413ABBAD631F233	05E4C4B1F258030690E6793C9C13C6F6AE234F68E5C41 236FDC919B7F589 032F	UniTrust Global TLS ECC Root CA R2
81	SHECA OV TLS ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA OV TLS ECC CA 2A O = UniTrust C = CN	A065578C43B2546C4E18DF86AED56725A9B7659C	08BA64405A3406C97BDCBD0E44224E6DD341F3EC93F1 368457DFA7CAC88 BE150	UniTrust Global TLS ECC Root CA R2
82	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	4BABE0E9328D5DAE17936F3DDAA2 442BFBDD0873F92FB8D1FBBD3D98 94649AD9	UniTrust Global TLS RSA Root CA R1
83	SHECA DV TLS RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA DV TLS RSA CA 1A O = UniTrust C = CN	C5E3A87F7EEDBC3E7108B34EF490EF2F2F1367D1	FFABEA74895DC0C78C224597472CF6937E0D740EF49DC2256C8E75A2A2A 15EDE	UniTrust Global TLS RSA Root CA R1
84	SHECA EV TLS RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA EV TLS RSA CA 1A O = UniTrust C = CN	60651A135EAB2B98A5A1041B3057A1D02FC612E5	B2525A5966CA68CA7F504F0A21FD73 847D174F89B48852A3E970588E1EAF C774	UniTrust Global TLS RSA Root CA R1
85	SHECA OV TLS RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA OV TLS RSA CA 1A O = UniTrust C = CN	F463091C1E2788B75DBBE91644B1744A34F34B46	7F8EF707C2D9A4B7D4ED5FDDC8AF4A64D99BF297D03 F8F01C4375DE74B 1C7DE1	UniTrust Global TLS RSA Root CA R1

pwc

羅兵咸永道

Attachment B - Publicly disclosed incidents

The list of incidents disclosed publicly during the period from April 1, 2023 to March 31, 2024 is as follow:

Bugzilla ID	Disclosure	Publicly Disclosed Link
1735908	SHECA: UniTrust: Improper DER results in failure to comply with RFC 5280 - Encoded sequence component with default value	Bugzilla Ticket Link
1814288	SHECA: Delayed revocation of intermediate CA certificates	Bugzilla Ticket Link
1815527	SHECA: organizationName problems in OV and EV TLS certificates	Bugzilla Ticket Link
1787537	UniTrust: EV certificate with wildcard domain in common name and SAN	Bugzilla Ticket Link
1798626	SHECA: UniTrust: EV certificate with wrong Registry Country Name	Bugzilla Ticket Link
1838765	SHECA: Outdated Organizational Units (OUs) problems in OV TLS certificates	Bugzilla Ticket Link
1838866	SHECA: Failure to Respond to April 2023 Survey	Bugzilla Ticket Link
1839105	SHECA: Non-compliant Subject Fields problem in OV TLS certificate	Bugzilla Ticket Link
1844799	SHECA: Failure to Submit Annual CCADB Self Assessment	Bugzilla Ticket Link
1855997	SHECA: CRLs not downloading	Bugzilla Ticket Link
1856503	SHECA: Failure to revoke within 5 days	Bugzilla Ticket Link
1859694	SHECA: Issuance of test certificates	Bugzilla Ticket Link

pwc 羅兵咸永道

注册会计师独立鉴证报告
（注意：本中文报告只作参考。正文请参阅英文报告。）

致：上海市数字证书认证中心有限公司（简称“SHECA”）管理层

范围

我们接受委托，对后附 SHECA 于 2023 年 4 月 1 日至 2024 年 3 月 31 日期间于中国上海（包括设施 1 和设施 2）运营的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证书认证业务规则 v3.7.7;
  - UniTrust证书认证业务规则 v3.7.6;
  - UniTrust证书认证业务规则 v3.7.5;
  - UniTrust证书认证业务规则 v3.7.4;
  - UniTrust证书认证业务规则 v3.7.3;
  - UniTrust证书认证业务规则 v3.7.2;
  - UniTrust证书策略 v1.5.5;
  - UniTrust证书策略 v1.5.4;
  - UniTrust证书策略 v1.5.3;
  - UniTrust证书策略 v1.5.2;
  - UniTrust证书策略 v1.5.1;
  - UniTrust证书策略 v1.5.0;
  - UniTrust事件证书策略&认证业务规则 v1.7;
  - UniTrust事件证书策略&认证业务规则 v1.6; 以及
  - UniTrust事件证书策略&认证业务规则 v1.5,

- 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
  - 中级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 v2.2.2。

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。

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。

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电子认证审计标准v2.2.2的规定。

我们的独立性和质量管理

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

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

注册会计师的责任

我们的责任是在执行鉴证工作的基础上对管理层认定发表意见。

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

合理保证的鉴证业务涉及实施鉴证程序，以获取有关管理层认定是否在所有重大方面符合 WebTrust 电子认证审计标准 v2.2.2 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 的内部控制的有效性和重要性，及其对用户及相关依赖方的控制风险评估所产生的影响，取决于控制间的相互作用以及其他存在于每个用户和相关依赖方的因素。我们并没有对用户和依赖方所负责的控制的有效性进行任何评估工作。

我们相信，我们获取的证据是充分、适当的，为发表鉴证意见提供了基础。

固有限制

由于内部控制体系本身的限制，SHECA 满足上述要求的能力可能会受到影响，例如：控制可能未达到预防、发现或纠正错误、舞弊、对系统或信息的未授权访问，或违反内外部制度或规定的要求。此外，风险的变化可能会影响本评估报告在将来时间的参考价值。

意见

我们认为，SHECA 于 2023 年 4 月 1 日至 2024 年 3 月 31 日期间的电子认证服务的管理层认定在所有重大方面符合 WebTrust 电子认证资格原则及规范 v2.2.2。

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 v2.2.2 以外的质量标准声明，或对任何客户对 SHECA 服务的合适性声明。

其他事项

UniTrust Global Root CA R1（附录 A#48），UniTrust Global Root CA R2（附录 A#55），UniTrust Global Root CA R3（附录 A#59）在 2023 年 4 月 1 日至 2024 年 3 月 31 日期间未颁发证书，仅保持在线以提供吊销状态信息。

在 2023 年 4 月 1 日至 2024 年 3 月 31 日期间，SHECA 管理层披露了 12 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。

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 电子认证审计标准 v2.2.2，因此 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 电子认证审计标准 v2.2.2 相关机构提交报告后，在 SHECA 网站上获取并展示 WebTrust Seal，不应向任何其它方分发或为其他目的使用。我们不会就本报告的内容向任何其他人士负上或承担任何责任。

WebTrust seal的使用

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

---

[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。*

羅兵咸永道

罗兵咸永道会计师事务所
注册会计师

香港，2024 年 5 月 24 日

附录 A：

下表列示了2023年4月1日至2024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 Root G2	Root Key	sha256RSA	2048 bits	CN = UCA Root G2 O = UniTrust C = CN	E4BB2C9FB2B51C8831AF7FCBDCF4052BE085F701	A07919A6391BCD6E15FB33A41B43A938EF3D19CF54F0198EC29D02364BC5A0EC	UCA Root G2
2	SHECA G2	Signing Key	sha256RSA	2048 bits	CN = SHECA G2 O = UniTrust C = CN	5688DEE3184382B772A426EB44A962D087C4AC26	69275DE8AF892E26E1B5339A664C194550799372F13CA6FB4966408F6A43C5B4	UCA Root G2
3	SHECA G2	Signing Key	sha256RSA	2048 bits	CN = SHECA G2 O = UniTrust C = CN	5688DEE3184382B772A426EB44A962D087C4AC26	23434A3078ADBE51DF267504F5655107ED1AA4E555D3DF21F479F1B4E4610A08	UCA Root G2
4	GlobalSign China CA for AATL	Signing Key	sha256RSA	2048 bits	CN = GlobalSign China CA for AATL O = GlobalSign China L = Shanghai S = Shanghai C = CN	FCAD8AADBF323AFF97C09BD74A7039888919D46A	D883436D97B08B008810D2EF3852D322E1D3528C751D3B23FF0C80803ED1CFAE	UCA Root G2
5	UCA Root SM2	Root Key	SM2	256 bits	CN = UCA Root SM2 O = UniTrust C = CN	EEE8B09CD5DCEC73FDEF7CFA502CC6C140E64CB3	307C77562B1532AE5FA6E63ED597CD54A0CBCC111F3598A7CCB2E19DD1351362	UCA Root SM2
6	UniTrust DV Secure Server CA G4	Signing Key	SM2	256 bits	CN = UniTrust DV Secure Server CA G4 O = UniTrust C = CN	ADA611696054F898CED269542A29DF239484E833	68B5E5FCA21925C5AF6628341FE6DBD187C6E66AEEF5F58295DCD7238FF56AD8	UCA Root SM2
7	UniTrust OV Secure Server CA G4	Signing Key	SM2	256 bits	CN = UniTrust OV Secure Server CA G4 O = UniTrust C = CN	D6546FA6587275420BF204794C4C6DE4368A8BD5	E75A9D14B5C5FF14779F0DC8A7889EE757788DC82706D95B4E2AF039098FA72C	UCA Root SM2
8	SHECA SM2	Signing Key	SM2	256 bits	CN = SHECA SM2 O = UniTrust C = CN	893104917B43AAAA9ABF841D9B86EEF0B87099A0	F5F6192276AED2141B3A66FD66724D46C5A58CACF618CAA5B5AA546ED5865207	UCA Root SM2

pwc

羅兵咸永道

#	密钥名称	密钥种类	密钥算法	密钥长度	主体识别名	密钥 ID	证书指纹（SHA256）	证书签发者
9	TrustAsia SM2 DV TLS CA - S1	Signing Key	SM2	256 bits	CN = TrustAsia SM2 DV TLS CA - S1 O = TrustAsia Technologies, Inc. C = CN	1B40CF756BB3E9D42B6AE0CCA449D5A26FE48F2A	FB812E1561383E0020103977D7E64D18B3587BC092F9DEC67600DE2A8493352C	UCA Root SM2
10	TrustAsia SM2 OV TLS CA - S1	Signing Key	SM2	256 bits	CN = TrustAsia SM2 OV TLS CA - S1 O = TrustAsia Technologies, Inc. C = CN	3623100989022D63A4C9E816BC531490AA2A01F7	2DBE68A196611EC658022F62607FBC0AA2000FD3147028EB2B16355B6D296EDF	UCA Root SM2
11	TrustAsia SM2 Identity CA - S1	Signing Key	SM2	256 bits	CN = TrustAsia SM2 Identity CA - S1 O = TrustAsia Technologies, Inc. C = CN	73075D5EFBF48320ED005F013AD1930E3FF432F2	BACE52158587138 8E4B3ECF44B5B4A965CCFD995C72D8813B61E643C77F1298D	UCA Root SM2
12	SHECA SM2 Identity CA G1	Signing Key	SM2	256 bits	CN = SHECA SM2 Identity CA G1 O = UniTrust C = CN	687C2F9B2E68A2DFCE11115411A6B60E6CEE2520	490BA44A5C4061D487EF1C945EC4889770A1F31299F0083045192D8978C25D7E	UCA Root SM2
13	CECloud Secure Server CA V1	Signing Key	SM2	256 bits	CN = CECloud Secure Server CA V1 O = 中国电子系统技术有限公司 C = CN	3D017054EBD1DAE2FA72558A7B4AD4112EC2789C	D973269DE727110F2577F12FC7039F204C8688F90479A60A6D918181E96BC921	UCA Root SM2
14	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	9BEA11C976FE014764C1BE56A6F914B5A560317ABD9988393382E5161AA0493C	UCA Global G2 Root
15	SHECA SMIME CA G1	Signing Key	sha256RSA	2048 bits	CN = SHECA SMIME CA G1 O = UniTrust C = CN	1FA80B4DCF9CA6A53ADAB096AB9957B90A9B7F5D	8100D384D6C4529883C37C37C68FD4903C41CCBCB9033A9C733A6AF0806E1DE7	UCA Global G2 Root
16	SHECA RSA Code Signing CA G3	Signing Key	sha256RSA	2048 bits	CN = SHECA RSA Code Signing CA G3 O = UniTrust C = CN	FD7EC87AC2771C5687D2AEF807C7426A1B7C42A8	C7E976AA77E92491C269840B2F1461E65147A2BB181EE59AB63BCD86704FE456	UCA Global G2 Root

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
17	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
18	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
19	SHECA RSA Time Stamp Authority G1	Signing Key	sha256RSA	2048 bits	CN = SHECA RSA Time Stamp Authority G1 O = UniTrust C = CN	6FC5770C4E825E4B544B30BD9933F408571A3DB4	86EE4A2F93137CA8887674078B394070F189B3049DD2D24053AE92924254C668	UCA Global G2 Root
20	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
21	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
22	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
23	SHECA Code Signing CA G4	Signing Key	sha256RSA	3072 bits	CN = SHECA Code Signing CA G4 O = UniTrust C = CN	73C3B39021CBF23BDA23D351F295C58BC678EE47	8F0C3E06A16E3EA7C9B15A848076ED15E51DA0B6F1AFA274EDE2B9102191FE0F	UCA Global G2 Root
24	SHECA Time Stamping CA G2	Signing Key	sha256RSA	3072 bits	CN = SHECA Time Stamping CA G2 O = UniTrust C = CN	CFDD9E670A6CB17E2C1A4F595387B2369BF96994	422C71F8DB9FDA2C65458B52363DB6FDC4E37B436774BCF97518F3F42EC725F1	UCA Global G2 Root
25	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

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
26	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
27	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
28	SHECA Global G3 Code Signing	Signing Key	sha256RSA	2048 bits	CN = SHECA Global G3 Code Signing O = UniTrust S = Shanghai C = CN	F73DF939A8D98754AC778EF5D995EEF835AB9439	EAA5AD8E9A2FA992354B2FF4254BEB08A632F7F17602604DDED58D73D616D844	UCA Global G2 Root
29	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
30	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
31	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	C1AFC65B1E813B0E6146E6AA5341681272ABE9A38D59F7BD1B27B729834A0D9C	Certum Trusted Network CA
32	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	3DD69C5BE170F943F804D1D31FE8F916C0C0226CDDD7AEA9AA9A0CDFD3474361	Certum Trusted Network CA
33	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	BB61408AED9F530B2EC0545E53BA2C8EBEAA57D9976447DB1663CED4600CD6B7	Certum Trusted Network CA
34	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	BFA95C5DF164B659FA32F6D10564D7170DDE661A853A782E6AB63639433BCB41	Certum Trusted Network CA

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
35	UCA Extended Validation Root	Root Key	sha256RSA	4096 bits	CN = UCA Extended Validation Root O = UniTrust C = CN	D9743AE4303D0DF712DC7E5A059F1E349AF7E114	D43AF9B35473755C9684FC06D7D8CB70EE5C28E773FB294EB41EE71722924D24	UCA Extended Validation Root
36	SHECA RSA Extended Validation Code Signing CA	Signing Key	sha256RSA	2048 bits	CN = SHECA RSA Extended Validation Code Signing CA O = UniTrust C = CN	8E40665F6AA940C2B9F1F04A22639564593707E5	D404FAFA4BA2F426B66CD219C6DA84F91C0FB7CB58429EC8077E2A764314D55D	UCA Extended Validation Root
37	SHECA RSA Extended Validation Server CA	Signing Key	sha256RSA	2048 bits	CN = SHECA RSA Extended Validation Server CA O = UniTrust C = CN	3B4B252A77372AFCB97FEDA8BDAF2299FC5DC5F4	4FD6FA527157EEA463689D7A4C2B934EF2222797254138 93D9847242C85CA9DF	UCA Extended Validation Root
38	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
39	SHECA EV Code Signing CA G2	Signing Key	sha256RSA	3072 bits	CN = SHECA EV Code Signing CA G2 O = UniTrust C = CN	5007CC4DF6F4BA37FC13CE1F2D22C956D89EA503	DD84169585A2E7A216AECD4083265A8EB51A64F7C6F1943671F8584C73F79A74	UCA Extended Validation Root
40	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
41	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
42	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
43	SHECA Extended Validation Code Signing CA	Signing Key	sha256RSA	2048 bits	CN = SHECA Extended Validation Code Signing CA O = UniTrust C = CN	7498996F6A15C0062520851CAF2B316B87EDA3DB	A392C645B9A5AD6A214F19DE776346BC7DD6BB15818E433886DAC54EE6661852	UCA Extended Validation Root

pwc

羅兵咸永道

#	密钥名称	密钥种类	密钥算法	密钥长度	主体识别名	密钥 ID	证书指纹（SHA256）	证书签发者
44	UniTrust Event Certificate Root CA R1	Root Key	sha384RSA	4096 bits	CN = UniTrust Event Certificate Root CA R1 O = UniTrust C = CN	D7418BEED45FC6E97D69108608AC7EE48BA0727E	3200B1BC5CF8F8BC0A382BD7809166A221600747DEC386D2625959CD75A28212	UniTrust Event Certificate Root CA R1
45	SHECA Event Certificate CA G1	Signing Key	sha256RSA	2048 bits	CN = SHECA Event Certificate CA G1 O = UniTrust C = CN	2A4D7575347FFFB46A57513816FFA99EEAAF0F4F	32AE6837AEF2DABBC8C19385A57A19FC97F6BDB8384B1ADCCDEAED3A891A3A0F	UniTrust Event Certificate Root CA R1
46	Orient Fortune Securities Co., Ltd Identity CA G1	Signing Key	sha256RSA	2048 bits	CN = Orient Fortune Securities Co., Ltd Identity CA G1 O = 东方财富证券股份有限公司 C = CN	8F155742AFDF87B618F8622DAB2E07091A796249	115250822139D3C6A49C821ABB19630FAC617190DAA3CF7373D3C95F082CBDF7	UniTrust Event Certificate Root CA R1
47	Shanghai Eastmoney Futures Co., Ltd. Identity CA G1	Signing Key	sha256RSA	2048 bits	CN = Shanghai Eastmoney Futures Co., Ltd Identity CA G1 O = 上海东方财富期货有限公司 C = CN	D09AE4CC4499268F8D72F83789C45F3F11B7BA8D	B4800869058B4B74CA970B3414FEDE2F676D90F979E4961325AD72B13ABE8866	UniTrust Event Certificate Root CA R1
48	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
49	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
50	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
51	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

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
52	SHECA Code Signing CA 1A	Signing Key	sha384RSA	4096 bits	CN = SHECA Code Signing CA 1A O = UniTrust C = CN	21B34B4FC6DD33246E861BACEBF182D7EFCA2CDA	59E3EF6680BCC0B1162DED4929D37E698C6A5CBEE075C03F1173AD653CF91CED	UniTrust Global Root CA R1
53	SHECA EV Code Signing CA 1A	Signing Key	sha384RSA	4096 bits	CN = SHECA EV Code Signing CA 1A O = UniTrust C = CN	510BE3C14EABDFEA38FF434E2C97339C0BFC27A9	03E04A3C2B5200BB27C679A37261852BAC7D46F3F371E4ECA80225AE288E4CFC	UniTrust Global Root CA R1
54	SHECA Time Stamping CA 1A	Signing Key	sha384RSA	4096 bits	CN = SHECA Time Stamping CA 1A O = UniTrust C = CN	8FBFB44A46F647EDF6EB8A0B5E1609430896FA46	2DFDBF6CEC0587B55F1300F109BC46EFD16BC7EB5F43CAE563953D87C7B432C4	UniTrust Global Root CA R1
55	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
56	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
57	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
58	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
59	UniTrust Global Root CA R3	Root Key	SM2	256 bits	CN = UniTrust Global Root CA R3 O = UniTrust C = CN	3B15E62B1C9F5015B64EA16D163A558AF4905FB5	6A19BCC7FAD2A5664F779BF143A72A2B079AC476E56FACBA48C352635CB4718F	UniTrust Global Root CA R3
60	SHECA DV Server CA 3A	Signing Key	SM2	256 bits	CN = SHECA DV Server CA 3A O = UniTrust C = CN	26924A66CDEDA9AD2DD7D0AE53C5DE95436A2C61	E464F2E140327DA8326C53A2FBA322F183E6DEFC56888A0811195265650BCAD1	UniTrust Global Root CA R3
61	SHECA OV Server CA 3A	Signing Key	SM2	256 bits	CN = SHECA OV Server CA 3A O = UniTrust C = CN	6F465A89CFB174BB558EB3A56D08093233E36D2F	19B057AB0827E37C8EB2EA7C04292068A253A3BEDC0C45848881C0BA78E717CF	UniTrust Global Root CA R3

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
62	SHECA EV Server CA 3A	Signing Key	SM2	256 bits	CN = SHECA EV Server CA 3A O = UniTrust C = CN	988B07A078C97576AF0CA1A723E87F4E9B482689	7F4A5FBCA47F8904D0AEA5D3BFA5759C4768BA6510EB1FEB5E5B076D12907741	UniTrust Global Root CA R3
63	UniTrust Global Code Signing ECC Root CA R2	Root Key	sha384ECDSA	384 bits	CN = UniTrust Global Code Signing ECC Root CA R2 O = UniTrust C = CN	D6E2F5C7B440515C5A3A5C490EFCB8C239503CDB	8854E81F9C6B47E438BBAE17E41F8BE4E68589AFD31A48BEE3F203F6DD3DA517	UniTrust Global Code Signing ECC Root CA R2
64	SHECA Code Signing ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA Code Signing ECC CA 2A O = UniTrust C = CN	3A5576122E385EB715671EE385BF1E3D0AC77A1A	953707AE07AF34970462E8C02AC3D10949D3684D063385277F31869508007D23	UniTrust Global Code Signing ECC Root CA R2
65	SHECA EV Code Signing ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA EV Code Signing ECC CA 2A O = UniTrust C = CN	BFAE7906E9776B61D01E4579986F2698B66DF25E	545BD126658352B306EE74185173F1774A79467A26E9BB6AE0ED44D86615DE5A	UniTrust Global Code Signing ECC Root CA R2
66	UniTrust Global Code Signing RSA Root CA R1	Root Key	sha384RSA	4096 bits	CN = UniTrust Global Code Signing RSA Root CA R1 O = UniTrust C = CN	60C14C87BDAAB27B678E4EA7921C519B481BA860	6357353A4BBCA3D5A158C95BE9DC90F0B3E2F6A6310FD5371FCB4C41E5E1BB4C	UniTrust Global Code Signing RSA Root CA R1
67	UniTrust Global SMIME ECC Root CA R2	Root Key	sha384ECDSA	384 bits	CN = UniTrust Global SMIME ECC Root CA R2 O = UniTrust C = CN	2D4D94407CFFC45D4357F190557448CF6CBEA343	6F4E2464D216A1E0B558BB204259B4A545AEB948957AA3EAF11B2F4DE1AFEF10	UniTrust Global SMIME ECC Root CA R2
68	SHECA IV SMIME ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA IV SMIME ECC CA 2A O = UniTrust C = CN	EBC1D6F67F2909A9928A90B4295818A02F3CAF1B	E82D794C1AC79F9BEBF3B6D98A237F84C15FD40C3ABB86C2214E699414F8FF54	UniTrust Global SMIME ECC Root CA R2
69	SHECA MV SMIME ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA MV SMIME ECC CA 2A O = UniTrust C = CN	FE0328035B693E5EDC5FAE0B742735DCC38C66F0	D7C4AB9D315AE8B889DA902C55264295D8CDC0F5471370490F4D4585E2C3C6D3	UniTrust Global SMIME ECC Root CA R2
70	SHECA OV SMIME ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA OV SMIME ECC CA 2A O = UniTrust C = CN	BD34144476B06D0F264C3CA9C349AC7153D4EF55	229B7FBCA2361DE63171067DE91DFFB3D2FA71A5ABE51CA41D5300C5750D2F0E	UniTrust Global SMIME ECC Root CA R2

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
71	UniTrust Global SMIME RSA Root CA R1	Root Key	sha384RSA	4096 bits	CN = UniTrust Global SMIME RSA Root CA R1 O = UniTrust C = CN	DF08E3E977C1F0FBF5F8D419504C7719F206CBA3	F0F255ADA2A643C0A1E7C8F54F3ED3DD25EF0E7378E76F7C127517ECFD952803	UniTrust Global SMIME RSA Root CA R1
72	SHECA IV SMIME RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA IV SMIME RSA CA 1A O = UniTrust C = CN	D38BCDC445B1E8D0AFDD8BE8E4A6B5B30A71EF4E	82BA6F1067468383757DF53F1628258043BBB972E1CAD31FD7AAD0ADD66A5B53	UniTrust Global SMIME RSA Root CA R1
73	SHECA MV SMIME RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA MV SMIME RSA CA 1A O = UniTrust C = CN	5A4AEFED9AE84052DA320BBB32C4E529ECDC5255	92148A115D26B287254B36164164B2220EE36B405D3B708CF5B7AB060C66B1FE	UniTrust Global SMIME RSA Root CA R1
74	SHECA OV SMIME RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA OV SMIME RSA CA 1A O = UniTrust C = CN	C061C3D053C9F412C5C9192DBB638305E4CA7EF8	6B661B964F2359C4CA68355243A2EEEDA9BACDA191D103A0C1119EC892018AC7	UniTrust Global SMIME RSA Root CA R1
75	UniTrust Global Time Stamping ECC Root CA R2	Root Key	sha384ECDSA	384 bits	CN = UniTrust Global Time Stamping ECC Root CA R2 O = UniTrust C = CN	C20E70D5E4015590A717B62DDDB5389D7627A1B7	90711D905CFF3C773A7320B5188A960C8A7D9E5966FA73284D64A4BF3E2FDA48	UniTrust Global Time Stamping ECC Root CA R2
76	SHECA Time Stamping ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA Time Stamping ECC CA 2A O = UniTrust C = CN	41315BE8FD8C3C65630168307A0B30EC097F1069	0E3FC096DDCC3205047F9042D57882A1144107243C47CDE6FFFDE403A5B7CA04	UniTrust Global Time Stamping ECC Root CA R2
77	UniTrust Global Time Stamping RSA Root CA R1	Root Key	sha384RSA	4096 bits	CN = UniTrust Global Time Stamping RSA Root CA R1 O = UniTrust C = CN	DA891E9DC30F38DAB0896CCDC5FDD7504F155B30	1759727D9E6679B069DD3AFA910E2779C42007AAB206A169C66E6E2A3D1774B0	UniTrust Global Time Stamping RSA Root CA R1
78	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	6C689FC6B014A1FB0CDEB5A3996171C15E728610602853 2E0210CEA8D9CD4E97	UniTrust Global TLS ECC Root CA R2
79	SHECA DV TLS ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA DV TLS ECC CA 2A O = UniTrust C = CN	CB65E62F50175F2C172B433F3A043CD213569A66	D690D8722EA89CD761790144952065 3339386AC4939F7EC5C1B195D9C3C95FA4	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
80	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
81	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
82	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
83	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
84	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
85	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2023年4月1日至2024年3月31日期间公开披露的事件：

Bugzilla ID	**事件名称**	**事件链接**
1735908	SHECA: UniTrust: Improper DER results in failure to comply with RFC 5280 - Encoded sequence component with default value	Bugzilla Ticket Link
1814288	SHECA: Delayed revocation of intermediate CA certificates	Bugzilla Ticket Link
1815527	SHECA: organizationName problems in OV and EV TLS certificates	Bugzilla Ticket Link
1787537	UniTrust: EV certificate with wildcard domain in common name and SAN	Bugzilla Ticket Link
1798626	SHECA: UniTrust: EV certificate with wrong Registry Country Name	Bugzilla Ticket Link
1838765	SHECA: Outdated Organizational Units (OUs) problems in OV TLS certificates	Bugzilla Ticket Link
1838866	SHECA: Failure to Respond to April 2023 Survey	Bugzilla Ticket Link
1839105	SHECA: Non-compliant Subject Fields problem in OV TLS certificate	Bugzilla Ticket Link
1844799	SHECA: Failure to Submit Annual CCADB Self Assessment	Bugzilla Ticket Link
1855997	SHECA: CRLs not downloading	Bugzilla Ticket Link
1856503	SHECA: Failure to revoke within 5 days	Bugzilla Ticket Link
1859694	SHECA: Issuance of test certificates	Bugzilla Ticket Link

Shanghai Electronic Certificate Authority Co.,Ltd

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

PricewaterhouseCoopers
22/F, Prince's Building, Central, Hong Kong

May 24, 2024

Dear Sirs,

Assertion of Management as to the Disclosure of Business Practices and Controls over the Certification Authority Operations during the period from April 1, 2023 through March 31, 2024

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

Facility 1 and Facility 2), China, throughout the period April 1, 2023 to March 31, 2024, SHECA has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environment control practices in its:
  - UniTrust Certification Practice Statement v3.7.7;
  - UniTrust Certification Practice Statement v3.7.6;
  - UniTrust Certification Practice Statement v3.7.5;
  - UniTrust Certification Practice Statement v3.7.4;
  - UniTrust Certification Practice Statement v3.7.3;
  - UniTrust Certification Practice Statement v3.7.2;
  - UniTrust Certificate Policy v1.5.5;
  - UniTrust Certificate Policy v1.5.4;
  - UniTrust Certificate Policy v1.5.3;
  - UniTrust Certificate Policy v1.5.2;
  - UniTrust Certificate Policy v1.5.1;
  - UniTrust Certificate Policy v1.5.0;
  - UniTrust Event Certification Policy & Certification Practice Statement v1.7;
  - UniTrust Event Certification Policy & Certification Practice Statement v1.6; and
  - UniTrust Event Certification Policy & Certification Practice Statement v1.5,

- maintained effective controls to provide reasonable assurance that:
  - SHECA's Certification Practice Statements are consistent with its Certificate Policies;
  - SHECA provides its services in accordance with its Certificate Policies and 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 v2.2.2, 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, Maintenance, and Change Management
- Disaster Recovery, Backups, and 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
- CA Key Destruction
- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management
- CA Key Migration

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

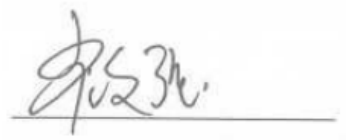
Subordinate CA Certificate Lifecycle Management Controls

- 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.

The UniTrust Global Root CA R1 (Appendix #48), UniTrust Global Root CA R2 (Appendix #55), UniTrust Global Root CA R3 (Appendix #59) CAs did not issue

certificates during the period April 1, 2023 to March 31, 2024 and were maintained online to provide revocation status information only.



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

Appendix

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

#	Key Name	Key Type	Signature Algorithm	Key Size	Subject DN	Subject Key Identifier	Certificates Thumbprint (SHA256)	Certificate Signed by
1	UCA Root G2	Root Key	sha256RSA	2048 bits	CN = UCA Root G2 O = UniTrust C = CN	E4BB2C9FB2B51C8831AF7FCBDCF4052BE085F701	A07919A6391BCD6E15FB33A41B43A938EF3D19CF54F0198EC29D02364BC5A0EC	UCA Root G2
2	SHECA G2	Signing Key	sha256RSA	2048 bits	CN = SHECA G2 O = UniTrust C = CN	5688DEE3184382B772A426EB44A962D087C4AC26	69275DE8AF892E26E1B5339A664C194550799372F13CA6FB4966408F6A43C5B4	UCA Root G2
3	SHECA G2	Signing Key	sha256RSA	2048 bits	CN = SHECA G2 O = UniTrust C = CN	5688DEE3184382B772A426EB44A962D087C4AC26	23434A3078ADBE51DF267504F5655107ED1AA4E555D3DF21F479F1B4E4610A08	UCA Root G2
4	GlobalSign China CA for AATL	Signing Key	sha256RSA	2048 bits	CN = GlobalSign China CA for AATL O = GlobalSign China L = Shanghai S = Shanghai C = CN	FCAD8AADBF323AFF97C09BD74A7039888919D46A	D883436D97B08B008810D2EF3852D322E1D3528C751D3B23FF0C80803ED1CFAE	UCA Root G2
5	UCA Root SM2	Root Key	SM2	256 bits	CN = UCA Root SM2 O = UniTrust C = CN	EEE8B09CD5DCEC73FDEF7CFA502CC6C140E64CB3	307C77562B1532AE5FA6E63ED597CD54A0CBCC111F3598A7CCB2E19DD1351362	UCA Root SM2
6	UniTrust DV Secure Server CA G4	Signing Key	SM2	256 bits	CN = UniTrust DV Secure Server CA G4 O = UniTrust C = CN	ADA611696054F898CED269542A29DF239484E833	68B5E5FCA21925C5AF6628341FE6DBD187C6E66AEEF5F58295DCD7238FF56AD8	UCA Root SM2
7	UniTrust OV Secure Server CA G4	Signing Key	SM2	256 bits	CN = UniTrust OV Secure Server CA G4 O = UniTrust C = CN	D6546FA6587275420BF204794C4C6DE4368A8BD5	E75A9D14B5C5FF14779F0DC8A7889EE757788DC82706D95B4E2AF039098FA72C	UCA Root SM2
8	SHECA SM2	Signing Key	SM2	256 bits	CN = SHECA SM2 O = UniTrust C = CN	893104917B43AAAA9ABF841D9B86EEF0B87099A0	F5F6192276AED2141B3A66FD66724D46C5A58CACF618CAA5B5AA546ED5865207	UCA Root SM2
9	TrustAsia SM2 DV TLS CA - S1	Signing Key	SM2	256 bits	CN = TrustAsia SM2 DV TLS CA - S1 O = TrustAsia Technologies, Inc. C = CN	1B40CF756BB3E9D42B6AE0CCA449D5A26FE48F2A	FB812E1561383E0020103977D7E64D18B3587BC092F9DEC67600DE2A8493352C	UCA Root SM2

#	Key Name	Key Type	Signature Algorithm	Key Size	Subject DN	Subject Key Identifier	Certificates Thumbprint (SHA256)	Certificate Signed by
10	TrustAsia SM2 OV TLS CA - S1	Signing Key	SM2	256 bits	CN = TrustAsia SM2 OV TLS CA - S1 O = TrustAsia Technologies, Inc. C = CN	3623100989022D63A4C9E816BC531490AA2A01F7	2DBE68A196611EC658022F62607FBC0AA2000FD3147028EB2B16355B6D296EDF	UCA Root SM2
11	TrustAsia SM2 Identity CA - S1	Signing Key	SM2	256 bits	CN = TrustAsia SM2 Identity CA - S1 O = TrustAsia Technologies, Inc. C = CN	73075D5EFBF48320ED005F013AD1930E3FF432F2	BACE52158587138E4B3ECF44B5B4A965CCFD995C72D8813B61E643C77F1298D	UCA Root SM2
12	SHECA SM2 Identity CA G1	Signing Key	SM2	256 bits	CN = SHECA SM2 Identity CA G1 O = UniTrust C = CN	687C2F9B2E68A2DFCE11115411A6B60E6CEE2520	490BA44A5C4061D487EF1C945EC4889770A1F31299F0083045192D8978C25D7E	UCA Root SM2
13	CECloud Secure Server CA V1	Signing Key	SM2	256 bits	CN = CECloud Secure Server CA V1 O = 中国电子系统技术有限公司 C = CN	3D017054EBD1DAE2FA72558A7B4AD4112EC2789C	D973269DE727110F2577F12FC7039F204C8688F90479A60A6D918181E96BC921	UCA Root SM2
14	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	9BEA11C976FE014764C1BE56A6F914B5A560317ABD9988393382E5161AA0493C	UCA Global G2 Root
15	SHECA SMIME CA G1	Signing Key	sha256RSA	2048 bits	CN = SHECA SMIME CA G1 O = UniTrust C = CN	1FA80B4DCF9CA6A53ADAB096AB9957B90A9B7F5D	8100D384D6C4529883C37C37C68FD4903C41CCBCB9033A9C733A6AF0806E1DE7	UCA Global G2 Root
16	SHECA RSA Code Signing CA G3	Signing Key	sha256RSA	2048 bits	CN = SHECA RSA Code Signing CA G3 O = UniTrust C = CN	FD7EC87AC2771C5687D2AEF807C7426A1B7C42A8	C7E976AA77E92491C269840B2F1461E65147A2BB181EE59AB63BCD86704FE456	UCA Global G2 Root
17	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
18	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

#	Key Name	Key Type	Signature Algorithm	Key Size	Subject DN	Subject Key Identifier	Certificates Thumbprint (SHA256)	Certificate Signed by
19	SHECA RSA Time Stamp Authority G1	Signing Key	sha256RSA	2048 bits	CN = SHECA RSA Time Stamp Authority G1 O = UniTrust C = CN	6FC5770C4E825E4B544B30BD9933F408571A3DB4	86EE4A2F93137CA8887674078B394070F189B3049DD2D24053AE92924254C668	UCA Global G2 Root
20	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
21	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
22	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
23	SHECA Code Signing CA G4	Signing Key	sha256RSA	3072 bits	CN = SHECA Code Signing CA G4 O = UniTrust C = CN	73C3B39021CBF23BDA23D351F295C58BC678EE47	8F0C3E06A16E3EA7C9B15A848076ED15E51DA0B6F1AFA274EDE2B9102191FE0F	UCA Global G2 Root
24	SHECA Time Stamping CA G2	Signing Key	sha256RSA	3072 bits	CN = SHECA Time Stamping CA G2 O = UniTrust C = CN	CFDD9E670A6CB17E2C1A4F595387B2369BF96994	422C71F8DB9FDA2C65458B52363DB6FDC4E37B436774BCF97518F3F42EC725F1	UCA Global G2 Root
25	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
26	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
27	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
28	SHECA Global G3 Code Signing	Signing Key	sha256RSA	2048 bits	CN = SHECA Global G3 Code Signing O = UniTrust S = Shanghai C = CN	F73DF939A8D98754AC778EF5D995EEF835AB9439	EAA5AD8E9A2FA992354B2FF4254BEB08A632F7F17602604DDED58D73D616D844	UCA Global G2 Root

#	Key Name	Key Type	Signature Algorithm	Key Size	Subject DN	Subject Key Identifier	Certificates Thumbprint (SHA256)	Certificate Signed by
29	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
30	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
31	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	C1AFC65B1E813B0E6146E6AA5341681272ABE9A38D59F7BD1B27B729834A0D9C	Certum Trusted Network CA
32	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	3DD69C5BE170F943F804D1D31FE8F916C0C0226CDDD7AEA9AA9A0CDFD3474361	Certum Trusted Network CA
33	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	BB61408AED9F530B2EC0545E53BA2C8EBEAA57D9976447DB1663CED4600CD6B7	Certum Trusted Network CA
34	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	BFA95C5DF164B659FA32F6D10564D7170DDE661A853A782E6AB63639433BCB41	Certum Trusted Network CA
35	UCA Extended Validation Root	Root Key	sha256RSA	4096 bits	CN = UCA Extended Validation Root O = UniTrust C = CN	D9743AE4303D0DF712DC7E5A059F1E349AF7E114	D43AF9B35473755C9684FC06D7D8CB70EE5C28E773FB294EB41EE71722924D24	UCA Extended Validation Root
36	SHECA RSA Extended Validation Code Signing CA	Signing Key	sha256RSA	2048 bits	CN = SHECA RSA Extended Validation Code Signing CA O = UniTrust C = CN	8E40665F6AA940C2B9F1F04A22639564593707E5	D404FAFA4BA2F426B66CD219C6DA84F91C0FB7CB58429EC8077E2A764314D55D	UCA Extended Validation Root
37	SHECA RSA Extended Validation Server CA	Signing Key	sha256RSA	2048 bits	CN = SHECA RSA Extended Validation Server CA O = UniTrust C = CN	3B4B252A77372AFCB97FEDA8BDAF2299FC5DC5F4	4FD6FA527157EEA463689D7A4C2B934EF2222797254138 93D9847242C85CA9DF	UCA Extended Validation Root
38	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

#	Key Name	Key Type	Signature Algorithm	Key Size	Subject DN	Subject Key Identifier	Certificates Thumbprint (SHA256)	Certificate Signed by
39	SHECA EV Code Signing CA G2	Signing Key	sha256RSA	3072 bits	CN = SHECA EV Code Signing CA G2 O = UniTrust C = CN	5007CC4DF6F4BA37FC13CE1F2D22C956D89EA503	DD84169585A2E7A216AECD4083265A8EB51A64F7C6F1943671F8584C73F79A74	UCA Extended Validation Root
40	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
41	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
42	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
43	SHECA Extended Validation Code Signing CA	Signing Key	sha256RSA	2048 bits	CN = SHECA Extended Validation Code Signing CA O = UniTrust C = CN	7498996F6A15C0062520851CAF2B316B87EDA3DB	A392C645B9A5AD6A214F19DE776346BC7DD6BB15818E433886DAC54EE6661852	UCA Extended Validation Root
44	UniTrust Event Certificate Root CA R1	Root Key	sha384RSA	4096 bits	CN = UniTrust Event Certificate Root CA R1 O = UniTrust C = CN	D7418BEED45FC6E97D69108608AC7EE48BA0727E	3200B1BC5CF8F8BC0A382BD7809166A221600747DEC386D2625959CD75A28212	UniTrust Event Certificate Root CA R1
45	SHECA Event Certificate CA G1	Signing Key	sha256RSA	2048 bits	CN = SHECA Event Certificate CA G1 O = UniTrust C = CN	2A4D7575347FFFB46A57513816FFA99EEAAF0F4F	32AE6837AEF2DABBC8C19385A57A19FC97F6BDB8384B1ADCCDEAED3A891A3A0F	UniTrust Event Certificate Root CA R1
46	Orient Fortune Securities Co., Ltd Identity CA G1	Signing Key	sha256RSA	2048 bits	CN = Orient Fortune Securities Co., Ltd Identity CA G1 O = 东方财富证券股份有限公司 C = CN	8F155742AFDF87B618F8622DAB2E07091A796249	115250822139D3C6A49C821ABB19630FAC617190DAA3CF7373D3C95F082CBDF7	UniTrust Event Certificate Root CA R1
47	Shanghai Eastmoney Futures Co., Ltd. Identity CA G1	Signing Key	sha256RSA	2048 bits	CN = Shanghai Eastmoney Futures Co., Ltd Identity CA G1 O = 上海东方财富期货有限公司 C = CN	D09AE4CC4499268F8D72F83789C45F3F11B7BA8D	B4800869058B4B74CA970B3414FEDE2F676D90F979E4961325AD72B13ABE8866	UniTrust Event Certificate Root CA R1

#	Key Name	Key Type	Signature Algorithm	Key Size	Subject DN	Subject Key Identifier	Certificates Thumbprint (SHA256)	Certificate Signed by
48	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
49	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
50	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
51	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
52	SHECA Code Signing CA 1A	Signing Key	sha384RSA	4096 bits	CN = SHECA Code Signing CA 1A O = UniTrust C = CN	21B34B4FC6DD33246E861BACEBF182D7EFCA2CDA	59E3EF6680BCC0B1162DED4929D37E698C6A5CBEE075C03F1173AD653CF91CED	UniTrust Global Root CA R1
53	SHECA EV Code Signing CA 1A	Signing Key	sha384RSA	4096 bits	CN = SHECA EV Code Signing CA 1A O = UniTrust C = CN	510BE3C14EABDFEA38FF434E2C97339C0BFC27A9	03E04A3C2B5200BB27C679A37261852BAC7D46F3F371E4ECA80225AE288E4CFC	UniTrust Global Root CA R1
54	SHECA Time Stamping CA 1A	Signing Key	sha384RSA	4096 bits	CN = SHECA Time Stamping CA 1A O = UniTrust C = CN	8FBFB44A46F647EDF6EB8A0B5E1609430896FA46	2DFDBF6CEC0587B55F1300F109BC46EFD16BC7EB5F43CAE563953D87C7B432C4	UniTrust Global Root CA R1
55	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
56	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
57	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
58	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

#	Key Name	Key Type	Signature Algorithm	Key Size	Subject DN	Subject Key Identifier	Certificates Thumbprint (SHA256)	Certificate Signed by
59	UniTrust Global Root CA R3	Root Key	SM2	256 bits	CN = UniTrust Global Root CA R3 O = UniTrust C = CN	3B15E62B1C9F5015B64EA16D163A558AF4905FB5	6A19BCC7FAD2A5664F779BF143A72A2B079AC476E56FACBA48C352635CB4718F	UniTrust Global Root CA R3
60	SHECA DV Server CA 3A	Signing Key	SM2	256 bits	CN = SHECA DV Server CA 3A O = UniTrust C = CN	26924A66CDEDA9AD2DD7D0AE53C5DE95436A2C61	E464F2E140327DA8326C53A2FBA322F183E6DEFC56888A0811195265650BCAD1	UniTrust Global Root CA R3
61	SHECA OV Server CA 3A	Signing Key	SM2	256 bits	CN = SHECA OV Server CA 3A O = UniTrust C = CN	6F465A89CFB174BB558EB3A56D08093233E36D2F	19B057AB0827E37C8EB2EA7C04292068A253A3BEDC0C45848881C0BA78E717CF	UniTrust Global Root CA R3
62	SHECA EV Server CA 3A	Signing Key	SM2	256 bits	CN = SHECA EV Server CA 3A O = UniTrust C = CN	988B07A078C97576AF0CA1A723E87F4E9B4822689	7F4A5FBCA47F8904D0AEA5D3BFA5759C4768BA6510EB1FEB5E5B076D12907741	UniTrust Global Root CA R3
63	UniTrust Global Code Signing ECC Root CA R2	Root Key	sha384ECDSA	384 bits	CN = UniTrust Global Code Signing ECC Root CA R2 O = UniTrust C = CN	D6E2F5C7B440515C5A3A5C490EFCB8C2395033CDB	8854E81F9C6B47E438BBAE17E41F8BE4E68589AFD31A48BEE3F203F6DD3DA517	UniTrust Global Code Signing ECC Root CA R2
64	SHECA Code Signing ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA Code Signing ECC CA 2A O = UniTrust C = CN	3A5576122E385EB715671EE385BF1E3D0AC77A1A	953707AE07AF34970462E8C02AC3D10949D3684D063385277F31869508007D23	UniTrust Global Code Signing ECC Root CA R2
65	SHECA EV Code Signing ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA EV Code Signing ECC CA 2A O = UniTrust C = CN	BFAE7906E9776B61D01E4579986F2698B66DF25E	545BD126658352B306EE74185173F1774A79467A26E9BB6AE0ED44D86615DE5A	UniTrust Global Code Signing ECC Root CA R2
66	UniTrust Global Code Signing RSA Root CA R1	Root Key	sha384RSA	4096 bits	CN = UniTrust Global Code Signing RSA Root CA R1 O = UniTrust C = CN	60C14C87BDAAB27B678E4EA7921C519B481BA860	6357353A4BBCA3D5A158C95BE9DC90F0B3E2F6A6310FD5371FCB4C41E5E1BB4C	UniTrust Global Code Signing RSA Root CA R1
67	UniTrust Global SMIME ECC Root CA R2	Root Key	sha384ECDSA	384 bits	CN = UniTrust Global SMIME ECC Root CA R2 O = UniTrust C = CN	2D4D94407CFFC45D4357F190557448CF6CBEA343	6F4E2464D216A1E0B558BB204259B4A545AEB948957AA3EAF11B2F4DE1AFEF10	UniTrust Global SMIME ECC Root CA R2
68	SHECA IV SMIME ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA IV SMIME ECC CA 2A O = UniTrust C = CN	EBC1D6F67F2909A9928A90B4295818A02F3CAF1B	E82D794C1AC79F9BEBF3B6D98A237F84C15FD40C3ABB86C2214E699414F8FF54	UniTrust Global SMIME ECC Root CA R2
69	SHECA MV SMIME ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA MV SMIME ECC CA 2A O = UniTrust C = CN	FE0328035B693E5EDC5FAE0B742735DCC38C66F0	D7C4AB9D315AE8B889DA902C55264295D8CDC0F5471370490F4D4585E2C3C6D3	UniTrust Global SMIME ECC Root CA R2

#	Key Name	Key Type	Signature Algorithm	Key Size	Subject DN	Subject Key Identifier	Certificates Thumbprint (SHA256)	Certificate Signed by
70	SHECA OV SMIME ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA OV SMIME ECC CA 2A O = UniTrust C = CN	BD34144476B06D0F264C3CA9C349AC7153D4EF55	229B7FBCA2361DE63171067DE91DFFB3D2FA71A5ABE51CA41D5300C5750D2F0E	UniTrust Global SMIME ECC Root CA R2
71	UniTrust Global SMIME RSA Root CA R1	Root Key	sha384RSA	4096 bits	CN = UniTrust Global SMIME RSA Root CA R1 O = UniTrust C = CN	DF08E3E977C1F0FBF5F8D419504C7719F206CBA3	F0F255ADA2A643C0A1E7C8F54F3ED3DD25EF0E7378E76F7C127517ECFD952803	UniTrust Global SMIME RSA Root CA R1
72	SHECA IV SMIME RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA IV SMIME RSA CA 1A O = UniTrust C = CN	D38BCDC445B1E8D0AFDD8BE8E4A6B5B30A71EF4E	82BA6F1067468383757DF53F1628258043BBB972E1CAD31FD7AAD0ADD66A5B53	UniTrust Global SMIME RSA Root CA R1
73	SHECA MV SMIME RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA MV SMIME RSA CA 1A O = UniTrust C = CN	5A4AEFED9AE84052DA320BBB32C4E529ECDC5255	92148A115D26B287254B36164164B2220EE36B405D3B708CF5B7AB060C66B1FE	UniTrust Global SMIME RSA Root CA R1
74	SHECA OV SMIME RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA OV SMIME RSA CA 1A O = UniTrust C = CN	C061C3D053C9F412C5C9192DBB638305E4CA7EF8	6B661B964F2359C4CA68355243A2EEEDA9BACDA191D103A0C1119EC892018AC7	UniTrust Global SMIME RSA Root CA R1
75	UniTrust Global Time Stamping ECC Root CA R2	Root Key	sha384ECDSA	384 bits	CN = UniTrust Global Time Stamping ECC Root CA R2 O = UniTrust C = CN	C20E70D5E4015590A717B62DDDB5389D7627A1B7	90711D905CFF3C773A7320B5188A960C8A7D9E5966FA73284D64A4BF3E2FDA48	UniTrust Global Time Stamping ECC Root CA R2
76	SHECA Time Stamping ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA Time Stamping ECC CA 2A O = UniTrust C = CN	41315BE8FD8C3C65630168307A0B30EC097F1069	0E3FC096DDCC3205047F9042D57882A1144107243C47CDE6FFFDE403A5B7CA04	UniTrust Global Time Stamping ECC Root CA R2
77	UniTrust Global Time Stamping RSA Root CA R1	Root Key	sha384RSA	4096 bits	CN = UniTrust Global Time Stamping RSA Root CA R1 O = UniTrust C = CN	DA891E9DC30F38DAB0896CCDC5FDD7504F155B30	1759727D9E6679B069DD3AFA910E2779C42007AAB206A169C66E6E2A3D1774B0	UniTrust Global Time Stamping RSA Root CA R1
78	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	6C689FC6B014A1FB0CDEB5A3996171C15E72861060285320E0210CEA8D9CD4E97	UniTrust Global TLS ECC Root CA R2
79	SHECA DV TLS ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA DV TLS ECC CA 2A O = UniTrust C = CN	CB65E62F50175F2C172B433F3A043CD213569A66	D690D8722EA89CD761790144952065 3339386AC4939F7EC5C1B195D9C3C95FA4	UniTrust Global TLS ECC Root CA R2
80	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

#	Key Name	Key Type	Signature Algorithm	Key Size	Subject DN	Subject Key Identifier	Certificates Thumbprint (SHA256)	Certificate Signed by
81	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
82	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
83	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
84	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
85	SHECA OV TLS RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA OV TLS RSA CA 1A O = UniTrust C = CN	F4630911C1E2788B75DBBE91644B1744A34F34B46	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

2024 年 5 月 24 日

致：罗兵咸永道会计师事务所

就 2023 年 4 月 1 日到 2024 年 3 月 31 日期间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（附录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
- 证书吊销
- 证书验证
- 订户密钥生成和管理
- 中级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 2023 年 4 月 1 日至 2024 年 3 月 31 日就 SHECA 在中国上海（包括设施 1 和设施 2）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证书认证业务规则 v3.7.7;
- UniTrust证书认证业务规则 v3.7.6;
- UniTrust证书认证业务规则 v3.7.5;
- UniTrust证书认证业务规则 v3.7.4;
- UniTrust证书认证业务规则 v3.7.3;
- UniTrust证书认证业务规则 v3.7.2;
- UniTrust证书策略 v1.5.5;
- UniTrust证书策略 v1.5.4;
- UniTrust证书策略 v1.5.3;
- UniTrust证书策略 v1.5.2;
- UniTrust证书策略 v1.5.1;
- UniTrust证书策略 v1.5.0;
- UniTrust事件证书策略&认证业务规则 v1.7;
- UniTrust事件证书策略&认证业务规则 v1.6; 以及
- UniTrust事件证书策略&认证业务规则 v1.5,

- 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
  - 中级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 v2.2.2, 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、维护与变更管理
- 灾难恢复、备份与业务连续性管理
- 监控与合规
- 审计日志

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
- CA密钥销毁
- CA密钥泄露
- CA加密设备生命周期管理
- CA密钥迁移

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
- 证书吊销
- 证书验证

中级CA证书生命周期管理

- 中级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。

UniTrust Global Root CA R1（附录#48），UniTrust Global Root CA R2（附录#55），UniTrust Global Root CA R3（附录#59）在 2023 年 4 月 1 日至 2024 年 3 月 31 日期间未颁发证书，仅保持在线以提供吊销状态信息。

_____

崔久强
上海市数字证书认证中心有限公司总经理

_____

公司盖章

附录

下表列示本管理层认定报告所包括的密钥和证书：

#	密钥名称	密钥种类	密钥算法	密钥长度	主体识别名	密钥 ID	证书指纹（SHA256）	证书签发者
1	UCA Root G2	Root Key	sha256RSA	2048 bits	CN = UCA Root G2 O = UniTrust C = CN	E4BB2C9FB2B51C8831AF7FCBDCF4052BE085F701	A07919A6391BCD6E15FB33A41B43A938EF3D19CF54F0198EC29D02364BC5A0EC	UCA Root G2
2	SHECA G2	Signing Key	sha256RSA	2048 bits	CN = SHECA G2 O = UniTrust C = CN	5688DEE3184382B772A426EB44A962D087C4AC26	69275DE8AF892E26E1B5339A664C194550799372F13CA6FB4966408F6A43C5B4	UCA Root G2
3	SHECA G2	Signing Key	sha256RSA	2048 bits	CN = SHECA G2 O = UniTrust C = CN	5688DEE3184382B772A426EB44A962D087C4AC26	23434A3078ADBE51DF267504F5655107ED1AA4E555D3DF21F479F1B4E4610A08	UCA Root G2
4	GlobalSign China CA for AATL	Signing Key	sha256RSA	2048 bits	CN = GlobalSign China CA for AATL O = GlobalSign China L = Shanghai S = Shanghai C = CN	FCAD8AADBF323AFF97C09BD74A7039888919D46A	D883436D97B08B008810D2EF3852D322E1D3528C751D3B23FF0C80803ED1CFAE	UCA Root G2
5	UCA Root SM2	Root Key	SM2	256 bits	CN = UCA Root SM2 O = UniTrust C = CN	EEE8B09CD5DCEC73FDEF7CFA502CC6C140E64CB3	307C77562B1532AE5FA6E63ED597CD54A0CBCC111F3598A7CCB2E19DD1351362	UCA Root SM2
6	UniTrust DV Secure Server CA G4	Signing Key	SM2	256 bits	CN = UniTrust DV Secure Server CA G4 O = UniTrust C = CN	ADA611696054F898CED269542A29DF239484E833	68B5E5FCA21925C5AF6628341FE6DBD187C6E66AEEF5F58295DCD7238FF56AD8	UCA Root SM2
7	UniTrust OV Secure Server CA G4	Signing Key	SM2	256 bits	CN = UniTrust OV Secure Server CA G4 O = UniTrust C = CN	D6546FA6587275420BF204794C4C6DE4368A8BD5	E75A9D14B5C5FF14779F0DC8A7889EE757788DC82706D95B4E2AF039098FA72C	UCA Root SM2
8	SHECA SM2	Signing Key	SM2	256 bits	CN = SHECA SM2 O = UniTrust C = CN	893104917B43AAAA9ABF841D9B86EEF0B87099A0	F5F6192276AED2141B3A66FD66724D46C5A58CACF618CAA5B5AA546ED5865207	UCA Root SM2
9	TrustAsia SM2 DV TLS CA - S1	Signing Key	SM2	256 bits	CN = TrustAsia SM2 DV TLS CA - S1 O = TrustAsia Technologies, Inc. C = CN	1B40CF756BB3E9D42B6AE0CCA449D5A26FE48F2A	FB812E1561383E0020103977D7E64D18B3587BC092F9DEC67600DE2A8493352C	UCA Root SM2

#	密钥名称	密钥种类	密钥算法	密钥长度	主体识别名	密钥 ID	证书指纹（SHA256）	证书签发者
10	TrustAsia SM2 OV TLS CA - S1	Signing Key	SM2	256 bits	CN = TrustAsia SM2 OV TLS CA - S1 O = TrustAsia Technologies, Inc. C = CN	3623100989022D63A4C9E816BC531490AA2A01F7	2DBE68A196611EC658022F62607FBC0AA2000FD3147028EB2B16355B6D296EDF	UCA Root SM2
11	TrustAsia SM2 Identity CA - S1	Signing Key	SM2	256 bits	CN = TrustAsia SM2 Identity CA - S1 O = TrustAsia Technologies, Inc. C = CN	73075D5EFBF48320ED005F013AD1930E3FF432F2	BACE52158587138 8E4B3ECF44B5B4A965CCFD995C72D8813B61E643C77F1298D	UCA Root SM2
12	SHECA SM2 Identity CA G1	Signing Key	SM2	256 bits	CN = SHECA SM2 Identity CA G1 O = UniTrust C = CN	687C2F9B2E68A2DFCE11115411A6B60E6CEE2520	490BA44A5C4061D487EF1C945EC4889770A1F31299F0083045192D8978C25D7E	UCA Root SM2
13	CECloud Secure Server CA V1	Signing Key	SM2	256 bits	CN = CECloud Secure Server CA V1 O = 中国电子系统技术有限公司 C = CN	3D017054EBD1DAE2FA72558A7B4AD4112EC2789C	D973269DE727110F2577F12FC7039F204C8688F90479A60A6D918181E96BC921	UCA Root SM2
14	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	9BEA11C976FE014764C1BE56A6F914B5A560317ABD9988393382E5161AA0493C	UCA Global G2 Root
15	SHECA SMIME CA G1	Signing Key	sha256RSA	2048 bits	CN = SHECA SMIME CA G1 O = UniTrust C = CN	1FA80B4DCF9CA6A53ADAB096AB9957B90A9B7F5D	8100D384D6C4529883C37C37C68FD4903C41CCBCB9033A9C733A6AF0806E1DE7	UCA Global G2 Root
16	SHECA RSA Code Signing CA G3	Signing Key	sha256RSA	2048 bits	CN = SHECA RSA Code Signing CA G3 O = UniTrust C = CN	FD7EC87AC2771C5687D2AEF807C7426A1B7C42A8	C7E976AA77E92491C269840B2F1461E65147A2BB181EE59AB63BCD86704FE456	UCA Global G2 Root
17	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
18	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

#	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
19	SHECA RSA Time Stamp Authority G1	Signing Key	sha256RSA	2048 bits	CN = SHECA RSA Time Stamp Authority G1 O = UniTrust C = CN	6FC5770C4E825E4B544B30BD9933F408571A3DB4	86EE4A2F93137CA8887674078B394070F189B3049DD2D24053AE92924254C668	UCA Global G2 Root
20	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
21	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
22	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
23	SHECA Code Signing CA G4	Signing Key	sha256RSA	3072 bits	CN = SHECA Code Signing CA G4 O = UniTrust C = CN	73C3B39021CBF23BDA23D351F295C58BC678EE47	8F0C3E06A16E3EA7C9B15A848076ED15E51DA0B6F1AFA274EDE2B9102191FE0F	UCA Global G2 Root
24	SHECA Time Stamping CA G2	Signing Key	sha256RSA	3072 bits	CN = SHECA Time Stamping CA G2 O = UniTrust C = CN	CFDD9E670A6CB17E2C1A4F595387B2369BF96994	422C71F8DB9FDA2C65458B52363DB6FDC4E37B436774BCF97518F3F42EC725F1	UCA Global G2 Root
25	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
26	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
27	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
28	SHECA Global G3 Code Signing	Signing Key	sha256RSA	2048 bits	CN = SHECA Global G3 Code Signing O = UniTrust S = Shanghai C = CN	F73DF939A8D98754AC778EF5D995EEF835AB9439	EAA5AD8E9A2FA992354B2FF4254BEB08A632F7F17602604DDED58D73D616D844	UCA Global G2 Root

#	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
29	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
30	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
31	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	C1AFC65B1E813B0E6146E6AA5341681272ABE9A38D59F7BD1B27B729834A0D9C	Certum Trusted Network CA
32	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	3DD69C5BE170F943F804D1D31FE8F916C0C0226CDDD7AEA9AA9A0CDFD3474361	Certum Trusted Network CA
33	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	BB61408AED9F530B2EC0545E53BA2C8EBEAA57D9976447DB1663CED4600CD6B7	Certum Trusted Network CA
34	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	BFA95C5DF164B659FA32F6D10564D7170DDE661A853A782E6AB63639433BCB41	Certum Trusted Network CA
35	UCA Extended Validation Root	Root Key	sha256RSA	4096 bits	CN = UCA Extended Validation Root O = UniTrust C = CN	D9743AE4303D0DF712DC7E5A059F1E349AF7E114	D43AF9B35473755C9684FC06D7D8CB70EE5C28E773FB294EB41EE71722924D24	UCA Extended Validation Root
36	SHECA RSA Extended Validation Code Signing CA	Signing Key	sha256RSA	2048 bits	CN = SHECA RSA Extended Validation Code Signing CA O = UniTrust C = CN	8E40665F6AA940C2B9F1F04A22639564593707E5	D404FAFA4BA2F426B66CD219C6DA84F91C0FB7CB58429EC8077E2A764314D55D	UCA Extended Validation Root
37	SHECA RSA Extended Validation Server CA	Signing Key	sha256RSA	2048 bits	CN = SHECA RSA Extended Validation Server CA O = UniTrust C = CN	3B4B252A77372AFCB97FEDA8BDAF2299FC5DC5F4	4FD6FA527157EEA463689D7A4C2B934EF2222797254138 93D9847242C85CA9DF	UCA Extended Validation Root
38	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

#	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
39	SHECA EV Code Signing CA G2	Signing Key	sha256RSA	3072 bits	CN = SHECA EV Code Signing CA G2 O = UniTrust C = CN	5007CC4DF6F4BA37FC13CE1F2D22C956D89EA503	DD84169585A2E7A216AECD4083265A8EB51A64F7C6F1943671F8584C73F79A74	UCA Extended Validation Root
40	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
41	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
42	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
43	SHECA Extended Validation Code Signing CA	Signing Key	sha256RSA	2048 bits	CN = SHECA Extended Validation Code Signing CA O = UniTrust C = CN	7498996F6A15C0062520851CAF2B316B87EDA3DB	A392C645B9A5AD6A214F19DE776346BC7DD6BB15818E433886DAC54EE6661852	UCA Extended Validation Root
44	UniTrust Event Certificate Root CA R1	Root Key	sha384RSA	4096 bits	CN = UniTrust Event Certificate Root CA R1 O = UniTrust C = CN	D7418BEED45FC6E97D69108608AC7EE48BA0727E	3200B1BC5CF8F8BC0A382BD7809166A221600747DEC386D2625959CD75A28212	UniTrust Event Certificate Root CA R1
45	SHECA Event Certificate CA G1	Signing Key	sha256RSA	2048 bits	CN = SHECA Event Certificate CA G1 O = UniTrust C = CN	2A4D7575347FFFB46A57513816FFA99EEAAF0F4F	32AE6837AEF2DABBC8C19385A57A19FC97F6BDB8384B1ADCCDEAED3A891A3A0F	UniTrust Event Certificate Root CA R1
46	Orient Fortune Securities Co., Ltd Identity CA G1	Signing Key	sha256RSA	2048 bits	CN = Orient Fortune Securities Co., Ltd Identity CA G1 O = 东方财富证券股份有限公司 C = CN	8F155742AFDF87B618F8622DAB2E07091A796249	115250822139D3C6A49C821ABB19630FAC617190DAA3CF7373D3C95F082CBDF7	UniTrust Event Certificate Root CA R1
47	Shanghai Eastmoney Futures Co., Ltd. Identity CA G1	Signing Key	sha256RSA	2048 bits	CN = Shanghai Eastmoney Futures Co., Ltd Identity CA G1 O = 上海东方财富期货有限公司 C = CN	D09AE4CC4499268F8D72F83789C45F3F11B7BA8D	B4800869058B4B74CA970B3414FEDE2F676D90F979E4961325AD72B13ABE8866	UniTrust Event Certificate 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
48	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
49	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
50	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
51	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
52	SHECA Code Signing CA 1A	Signing Key	sha384RSA	4096 bits	CN = SHECA Code Signing CA 1A O = UniTrust C = CN	21B34B4FC6DD33246E861BACEBF182D7EFCA2CDA	59E3EF6680BCC0B1162DED4929D37E698C6A5CBEE075C03F1173AD653CF91CED	UniTrust Global Root CA R1
53	SHECA EV Code Signing CA 1A	Signing Key	sha384RSA	4096 bits	CN = SHECA EV Code Signing CA 1A O = UniTrust C = CN	510BE3C14EABDFEA38FF434E2C97339C0BFC27A9	03E04A3C2B5200BB27C679A37261852BAC7D46F3F371E4ECA80225AE288E4CFC	UniTrust Global Root CA R1
54	SHECA Time Stamping CA 1A	Signing Key	sha384RSA	4096 bits	CN = SHECA Time Stamping CA 1A O = UniTrust C = CN	8FBFB44A46F647EDF6EB8A0B5E1609430896FA46	2DFDBF6CEC0587B55F1300F109BC46EFD16BC7EB5F43CAE563953D87C7B432C4	UniTrust Global Root CA R1
55	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
56	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
57	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
58	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
59	UniTrust Global Root CA R3	Root Key	SM2	256 bits	CN = UniTrust Global Root CA R3 O = UniTrust C = CN	3B15E62B1C9F5015B64EA16D163A558AF4905FB5	6A19BCC7FAD2A5664F779BF143A72A2B079AC476E56FACBA48C352635CB4718F	UniTrust Global Root CA R3

#	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
60	SHECA DV Server CA 3A	Signing Key	SM2	256 bits	CN = SHECA DV Server CA 3A O = UniTrust C = CN	26924A66CDEDA9AD2DD7D0AE53C5DE95436A2C61	E464F2E140327DA8326C53A2FBA322F183E6DEFC56888A0811195265650BCAD1	UniTrust Global Root CA R3
61	SHECA OV Server CA 3A	Signing Key	SM2	256 bits	CN = SHECA OV Server CA 3A O = UniTrust C = CN	6F465A89CFB174BB558EB3A56D08093233E36D2F	19B057AB0827E37C8EB2EA7C04292068A253A3BEDC0C45848881C0BA78E717CF	UniTrust Global Root CA R3
62	SHECA EV Server CA 3A	Signing Key	SM2	256 bits	CN = SHECA EV Server CA 3A O = UniTrust C = CN	988B07A078C97576AF0CA1A723E87F4E9B482689	7F4A5FBCA47F8904D0AEA5D3BFA5759C4768BA6510EB1FEB5E5B076D12907741	UniTrust Global Root CA R3
63	UniTrust Global Code Signing ECC Root CA R2	Root Key	sha384ECDSA	384 bits	CN = UniTrust Global Code Signing ECC Root CA R2 O = UniTrust C = CN	D6E2F5C7B440515C5A3A5C490EFCB8C2395033CDB	8854E81F9C6B47E438BBAE17E41F8BE4E68589AFD31A48BEE3F203F6DD3DA517	UniTrust Global Code Signing ECC Root CA R2
64	SHECA Code Signing ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA Code Signing ECC CA 2A O = UniTrust C = CN	3A5576122E385EB715671EE385BF1E3D0AC77A1A	953707AE07AF34970462E8C02AC3D10949D3684D063385277F31869508007D23	UniTrust Global Code Signing ECC Root CA R2
65	SHECA EV Code Signing ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA EV Code Signing ECC CA 2A O = UniTrust C = CN	BFAE7906E9776B61D01E4579986F2698B66DF25E	545BD126658352B306EE74185173F1774A79467A26E9BB6AE0ED44D86615DE5A	UniTrust Global Code Signing ECC Root CA R2
66	UniTrust Global Code Signing RSA Root CA R1	Root Key	sha384RSA	4096 bits	CN = UniTrust Global Code Signing RSA Root CA R1 O = UniTrust C = CN	60C14C87BDAAB27B678E4EA7921C519B481BA860	6357353A4BBCA3D5A158C95BE9DC90F0B3E2F6A6310FD5371FCB4C41E5E1BB4C	UniTrust Global Code Signing RSA Root CA R1
67	UniTrust Global SMIME ECC Root CA R2	Root Key	sha384ECDSA	384 bits	CN = UniTrust Global SMIME ECC Root CA R2 O = UniTrust C = CN	2D4D94407CFFC45D4357F190557448CF6CBEA343	6F4E2464D216A1E0B558BB204259B4A545AEB948957AA3EAF11B2F4DE1AFEF10	UniTrust Global SMIME ECC Root CA R2
68	SHECA IV SMIME ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA IV SMIME ECC CA 2A O = UniTrust C = CN	EBC1D6F67F2909A9928A90B4295818A02F3CAF1B	E82D794C1AC79F9BEBF3B6D98A237F84C15FD40C3ABB86C2214E699414F8FF54	UniTrust Global SMIME ECC Root CA R2
69	SHECA MV SMIME ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA MV SMIME ECC CA 2A O = UniTrust C = CN	FE0328035B693E5EDC5FAE0B742735DCC38C66F0	D7C4AB9D315AE8B889DA902C55264295D8CDC0F5471370490F4D4585E2C3C6D3	UniTrust Global SMIME ECC Root CA R2
70	SHECA OV SMIME ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA OV SMIME ECC CA 2A O = UniTrust C = CN	BD34144476B06D0F264C3CA9C349AC7153D4EF55	229B7FBCA2361DE63171067DE91DFFB3D2FA71A5ABE51CA41D5300C5750D2F0E	UniTrust Global SMIME ECC Root CA R2

#	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
71	UniTrust Global SMIME RSA Root CA R1	Root Key	sha384RSA	4096 bits	CN = UniTrust Global SMIME RSA Root CA R1 O = UniTrust C = CN	DF08E3E977C1F0FBF5F8D419504C7719F206CBA3	F0F255ADA2A643C0A1E7C8F54F3ED3DD25EF0E7378E76F7C127517ECFD952803	UniTrust Global SMIME RSA Root CA R1
72	SHECA IV SMIME RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA IV SMIME RSA CA 1A O = UniTrust C = CN	D38BCDC445B1E8D0AFDD8BE8E4A6B5B30A71EF4E	82BA6F1067468383757DF53F1628258043BBB972E1CAD31FD7AAD0ADD66A5B53	UniTrust Global SMIME RSA Root CA R1
73	SHECA MV SMIME RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA MV SMIME RSA CA 1A O = UniTrust C = CN	5A4AEFED9AE84052DA320BBB32C4E529ECDC5255	92148A115D26B287254B36164164B2220EE36B405D3B708CF5B7AB060C66B1FE	UniTrust Global SMIME RSA Root CA R1
74	SHECA OV SMIME RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA OV SMIME RSA CA 1A O = UniTrust C = CN	C061C3D053C9F412C5C9192DBB638305E4CA7EF8	6B661B964F2359C4CA68355243A2EEEDA9BACDA191D103A0C1119EC892018AC7	UniTrust Global SMIME RSA Root CA R1
75	UniTrust Global Time Stamping ECC Root CA R2	Root Key	sha384ECDSA	384 bits	CN = UniTrust Global Time Stamping ECC Root CA R2 O = UniTrust C = CN	C20E70D5E4015590A717B62DDDB5389D7627A1B7	90711D905CFF3C773A7320B5188A960C8A7D9E5966FA73284D64A4BF3E2FDA48	UniTrust Global Time Stamping ECC Root CA R2
76	SHECA Time Stamping ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA Time Stamping ECC CA 2A O = UniTrust C = CN	41315BE8FD8C3C65630168307A0B30EC097F1069	0E3FC096DDCC3205047F9042D57882A1144107243C47CDE6FFFDE403A5B7CA04	UniTrust Global Time Stamping ECC Root CA R2
77	UniTrust Global Time Stamping RSA Root CA R1	Root Key	sha384RSA	4096 bits	CN = UniTrust Global Time Stamping RSA Root CA R1 O = UniTrust C = CN	DA891E9DC30F38DAB0896CCDC5FDD7504F155B30	1759727D9E6679B069DD3AFA910E2779C42007AAB206A169C66E6E2A3D1774B0	UniTrust Global Time Stamping RSA Root CA R1
78	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	6C689FC6B014A1FB0CDEB5A3996171C15E728610602853 2E0210CEA8D9CD4E97	UniTrust Global TLS ECC Root CA R2
79	SHECA DV TLS ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA DV TLS ECC CA 2A O = UniTrust C = CN	CB65E62F50175F2C172B433F3A043CD213569A66	D690D8722EA89CD761790144952065 3339386AC4939F7EC5C1B195D9C3C95FA4	UniTrust Global TLS ECC Root CA R2
80	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
81	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

#	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
82	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
83	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
84	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
85	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