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 locations as enumerated in Attachment C, for the period from April 1, 2025 to March 31, 2026 for its CAs as enumerated in Attachment A, SHECA has:

- disclosed its S/MIME certificate lifecycle management business practices in its Certificate Policies/Certification Practice Statements ("CP"/ "CPS") enumerated in Attachment B, including its commitment to provide S/MIME certificates in conformity with the CA/Browser Forum Requirements on the SHECA website, and provided such services in accordance with its disclosed practices,
- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and S/MIME certificates it manages is established and protected throughout their lifecycles; and
  - S/MIME subscriber information is properly authenticated (for the registration activities performed by SHECA),
- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorized individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity,

in accordance with the WebTrust Principles and Criteria for Certification Authorities – S/MIME Certificates v1.0.13.

The CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted

PricewaterhouseCoopers, 22/F, Prince's Building, Central, Hong Kong
T: +852 2289 8888, F:+852 2810 9888

S/MIME Certificates require the CA to operate controls to adhere to the Network and Certificate System Security Requirements. The WebTrust Principles and Criteria for Certification Authorities – Network Security address this requirement and are reported on in a separate report.

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 – S/MIME Certificates v1.0.13.

Our Independence and Quality Management

We have complied with the independence and other ethical requirements of the Code of Ethics for Professional Accountants as issued by the Hong Kong Institute of Certified Public Accountants (the "HKICPA"), which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

Our firm applies Hong Kong Standard on Quality Management 1 as issued by the HKICPA, 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 Hong Kong Standard on Assurance Engagements 3000 (Revised) "Assurance Engagements Other Than Audits or Reviews of Historical Financial Information" issued by the HKICPA. 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 – S/MIME Certificates v1.0.13. 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 S/MIME certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of S/MIME

certificates; (2) selectively testing transactions executed in accordance with disclosed S/MIME 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, 2025 to March 31, 2026, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities – S/MIME Certificates v1.0.13.

Emphasis of Matter

We draw attention to the fact that this report does not include any representation as to the quality of SHECA's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – S/MIME Certificates v1.0.13, nor the suitability of any of SHECA's services for any customer's intended purpose. Our opinion is not modified in respect of this matter.

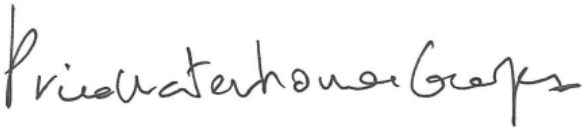
Purpose and Restriction on Use

The management's assertion was prepared for obtaining and displaying the WebTrust Seal on SHECA website[1] using the WebTrust Principles and Criteria for Certification Authorities – S/MIME Certificates v1.0.13 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 – S/MIME Certificates v1.0.13.

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 – S/MIME Certificates 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, June 10, 2026

[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.

Attachment A

The list of CAs and certificates in scope for the period from April 1, 2025 to March 31, 2026 is as follow:

Root CAs

#	CA Name	Key Type	Signature Algorithm	Key Size	Subject DN	Subject Key Identifier	Certificates Thumbprint (SHA256)	Certificate Signed by
1	UniTrust Global SMIME RSA Root CA R1	Root Key	sha384RSA	4096 bits	CN = UniTrust Global SMIME RSA Root CA R1 O = UniTrust C = CN	2E7C233EDD6396A24449FEAC6CB82388B8C868F3	F0F255ADA2A643C0A1E7C8F54F3ED3DD25EF0E7378E76F7C127517ECFD952803	UniTrust Global SMIME RSA Root CA R1
2	UniTrust Global SMIME ECC Root CA R2	Root Key	sha384ECDSA	384 bits	CN = UniTrust Global SMIME ECC Root CA R2 O = UniTrust C = CN	019FFAAC3E116DFE4D7A3912205EF40985313E4C	6F4E2464D216A1E0B558BB204259B4A545AEB948957AA3EAF11B2F4DE1AFEF10	UniTrust Global SMIME ECC Root CA R2
3	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	9BEA11C976FE014764C1BE56A6F914B5A560317ABD9988393382E5161AA0493C	UCA Global G2 Root

Cross-signed CAs

#	CA Name	Key Type	Signature Algorithm	Key Size	Subject DN	Subject Key Identifier	Certificates Thumbprint (SHA256)	Certificate Signed by
4	UniTrust Global TLS ECC Root CA R2	Signing Key	sha384RSA	384 bits	CN = UniTrust Global TLS ECC Root CA R2 O = UniTrust C = CN	46E3D4F8DF88838AB7AE69966E00526FBB43D791	8ED6FA47B14DC79C85ED5C4CE2C67B2F2F96D2B9054690F28BF2DFE9A5770DF0	UCA Global G2 Root
5	UniTrust Global TLS ECC Root CA R2	Signing Key	sha384RSA	384 bits	CN = UniTrust Global TLS ECC Root CA R2 O = UniTrust C = CN	46E3D4F8DF88838AB7AE69966E00526FBB43D791	F2384371C93EB284166FD07A34F211FAA697B6FC20D4D31F7A8E4A3283CA3FF1	UCA Global G2 Root
6	UniTrust Global TLS RSA Root CA R1	Signing Key	sha384RSA	4096 bits	CN = UniTrust Global TLS RSA Root CA R1 O = UniTrust C = CN	E349C5A5003582FB630CBB369A86E24C4185DB08	E4C25DE1B285B3C45358EF12583A1AA78DB148D0D294F8798339451FC1910542	UCA Global G2 Root
7	UniTrust Global TLS RSA Root CA R1	Signing Key	sha384RSA	4096 bits	CN = UniTrust Global TLS RSA Root CA R1	E349C5A5003582FB630CBB369A86E24C4185DB08	50404B08111323C691E1695737556E4AFCDCC87EADD22C5503B6D03392AADDDF	UCA Global G2 Root

#	CA Name	Key Type	Signature Algorithm	Key Size	Subject DN	Subject Key Identifier	Certificates Thumbprint (SHA256)	Certificate Signed by
					O = UniTrust C = CN			
8	UCA Global G2 Root	Signing Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	BB61408AED9F530B2EC0545E53BA2C8EBEAA57D9976447DB1663CED4600CD6B7	Certum Trusted Network CA
9	UCA Global G2 Root	Signing Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	BFA95C5DF164B659FA32F6D10564D7170DDE661A853A782E6AB63639433BCB41	Certum Trusted Network CA

Sub CAs

#	CA Name	Key Type	Signature Algorithm	Key Size	Subject DN	Subject Key Identifier	Certificates Thumbprint (SHA256)	Certificate Signed by
10i	SHECA IV SMIME RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA IV SMIME RSA CA 1A O = UniTrust C = CN	0731D082BC0A0AEF2F464617AF73F5C05E3976BE	82BA6F1067468383757DF53F1628258043BBB972E1CAD31FD7AAD0ADD66A5B53	UniTrust Global SMIME RSA Root CA R1
11	SHECA MV SMIME RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA MV SMIME RSA CA 1A O = UniTrust C = CN	838975C497C317A6532B73F31C7FBCAEA2FE1E90	92148A115D26B287254B36164164B2220EE36B405D3B708CF5B7AB060C66B1FE	UniTrust Global SMIME RSA Root CA R1
12	SHECA OV SMIME RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA OV SMIME RSA CA 1A O = UniTrust C = CN	82964C637D30CB2841C53AC7E84D1EB99489FF5A	6B661B964F2359C4CA68355243A2EEEDA9BACDA191D103A0C1119EC892018AC7	UniTrust Global SMIME RSA Root CA R1
13	SHECA IV SMIME ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA IV SMIME ECC CA 2A O = UniTrust C = CN	983BC3F8CEA554065FB1CD3F99F4B76AB2C22EC5	E82D794C1AC79F9BEBF3B6D98A237F84C15FD40C3ABB86C2214E699414F8FF54	UniTrust Global SMIME ECC Root CA R2
14	SHECA MV SMIME ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA MV SMIME ECC CA 2A O = UniTrust C = CN	D9B98D06C0DBD56A3497D7A9B0E9AE8B61B9F032	D7C4AB9D315AE8B889DA902C55264295D8CDC0F5471370490F4D4585E2C3C6D3	UniTrust Global SMIME ECC Root CA R2
15	SHECA OV SMIME ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA OV SMIME ECC CA 2A O = UniTrust C = CN	1CD15D6061277F084A21AD9518E43191D639DC18	229B7FBCA2361DE63171067DE91DFFB3D2FA71A5ABE51CA41D5300C5750D2F0E	UniTrust Global SMIME ECC Root CA R2
16	SHECA SMIME CA G1	Signing Key	sha256RSA	2048 bits	CN = SHECA SMIME CA G1	1FA80B4DCF9CA6A53ADAB096AB9957B90A9B7F5D	8100D384D6C4529883C37C37C68FD4903C41CCBCB9033A9C733A6AF0806E1DE7	UCA Global G2 Root

#	CA Name	Key Type	Signature Algorithm	Key Size	Subject DN	Subject Key Identifier	Certificates Thumbprint (SHA256)	Certificate Signed by
					O = UniTrust C = CN			
17	SHECA MV SMIME RSA CA G1	Signing Key	sha384RSA	3072 bits	CN = SHECA MV SMIME RSA CA G1 O = UniTrust C = CN	4F111E8FD4506500D7CE565190AF012BFB143845	C064FAB74E8723164932A25CFB6708106E1E5A3A05CFD1079B1DCF52792C5908	UCA Global G2 Root
18	SHECA IV SMIME RSA CA G1	Signing Key	sha384RSA	3072 bits	CN = SHECA IV SMIME RSA CA G1 O = UniTrust C = CN	E010A54E644A8F605F134C5C108E742C0168BBE5	2A1AAA3E4D7C6EC8BE083BDBDD247153A88D51F1226FD9691B872AE23D166BFF	UCA Global G2 Root
19	SHECA OV SMIME RSA CA G1	Signing Key	sha384RSA	3072 bits	CN = SHECA OV SMIME RSA CA G1 O = UniTrust C = CN	E3B8865D1EF2FF2146219648BD54022EC93BC85C	73BA9F7AE0924F3567F0280568A7050A58C9C4855DE0686C2FDC48522EB86D2D	UCA Global G2 Root

Attachment B

The list of SHECA's Certification Practice Statements in scope for the period from April 1, 2025 to March 31, 2026 is as follow:

Policy Name	Version
UniTrust Certification Practice Statement	V3.8.2
	V3.8.1
	V3.8.0
	V3.7.9
UniTrust Certificate Policy	V1.6
	V1.5.9
	V1.5.8
	V1.5.7
SHECA SMIME CP/CPS	V1.1
	V1.0

Attachment C

The list of CA locations in scope for the period from April 1, 2025 to March 31, 2026 is as follow:

Location Name	Location	In-Scope for Physical and Environmental Control Testing
Facility 1	Shanghai, China	Yes
Facility 2	Shanghai, China	Yes
Facility 3	Shanghai, China	Yes

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/

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

The management of SHECA is responsible for establishing and maintaining effective controls over its S/MIME CA operations, including its S/MIME CA business practices disclosure on its website, S/MIME key lifecycle management controls, and S/MIME 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 S/MIME CA services. Based on that assessment, in providing its S/MIME CA services at Shanghai (including Facility 1, Facility 2 and Facility 3), China, throughout the period April 1, 2025 to March 31, 2026, SHECA has:

- disclosed its S/MIME certificate lifecycle management business practices in its Certificate Policies/Certification Practice Statements ("CP"/ "CPS") enumerated in Attachment B, including its commitment to provide S/MIME certificates in conformity with the CA/Browser Forum Requirements on the SHECA website, and provided such services in accordance with its disclosed practices

- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and S/MIME certificates it manages is established and protected throughout their lifecycles; and

- S/MIME subscriber information is properly authenticated (for the registration activities performed by SHECA),

- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorized individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity,

in accordance with the WebTrust Principles and Criteria for Certification Authorities – S/MIME Certificates v1.0.13.

Mr. Cui Jiuqiang
General Manager of Shanghai Electronic Certificate Authority Co., Ltd.
June 10, 2026

Attachment A

The list of CAs and certificates covered in the management's assertion for the period from April 1, 2025 to March 31, 2026 is as follow:

Root CAs

#	CA Name	Key Type	Signature Algorithm	Key Size	Subject DN	Subject Key Identifier	Certificates Thumbprint (SHA256)	Certificate Signed by
1	UniTrust Global SMIME RSA Root CA R1	Root Key	sha384RSA	4096 bits	CN = UniTrust Global SMIME RSA Root CA R1 O = UniTrust C = CN	2E7C233EDD6396A24449FEAC6CB82388B8C868F3	F0F255ADA2A643C0A1E7C8F54F3ED3DD25EF0E7378E76F7C127517ECFD952803	UniTrust Global SMIME RSA Root CA R1
2	UniTrust Global SMIME ECC Root CA R2	Root Key	sha384ECDSA	384 bits	CN = UniTrust Global SMIME ECC Root CA R2 O = UniTrust C = CN	019FFAAC3E116DFE4D7A3912205EF40985313E4C	6F4E2464D216A1E0B558BB204259B4A545AEB948957AA3EAF11B2F4DE1AFEF10	UniTrust Global SMIME ECC Root CA R2
3	UCA Global G2 Root	Root Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	9BEA11C976FE014764C1BE56A6F914B5A560317ABD9988393382E5161AA0493C	UCA Global G2 Root

Cross-signed CAs

#	CA Name	Key Type	Signature Algorithm	Key Size	Subject DN	Subject Key Identifier	Certificates Thumbprint (SHA256)	Certificate Signed by
4	UniTrust Global TLS ECC Root CA R2	Signing Key	sha384RSA	384 bits	CN = UniTrust Global TLS ECC Root CA R2 O = UniTrust C = CN	46E3D4F8DF88838AB7AE69966E00526FBB43D791	8ED6FA47B14DC79C85ED5C4CE2C67B2F2F96D2B9054690F28BF2DFE9A5770DF0	UCA Global G2 Root
5	UniTrust Global TLS ECC Root CA R2	Signing Key	sha384RSA	384 bits	CN = UniTrust Global TLS ECC Root CA R2 O = UniTrust C = CN	46E3D4F8DF88838AB7AE69966E00526FBB43D791	F2384371C93EB284166FD07A34F211FAA697B6FC20D4D31F7A8E4A3283CA3FF1	UCA Global G2 Root
6	UniTrust Global TLS RSA Root CA R1	Signing Key	sha384RSA	4096 bits	CN = UniTrust Global TLS RSA Root CA R1 O = UniTrust C = CN	E349C5A5003582FB630CBB369A86E24C4185DB08	E4C25DE1B285B3C45358EF12583A1AA78DB148D0D294F8798339451FC1910542	UCA Global G2 Root

#	CA Name	Key Type	Signature Algorithm	Key Size	Subject DN	Subject Key Identifier	Certificates Thumbprint (SHA256)	Certificate Signed by
7	UniTrust Global TLS RSA Root CA R1	Signing Key	sha384RSA	4096 bits	CN = UniTrust Global TLS RSA Root CA R1 O = UniTrust C = CN	E349C5A5003582FB630CBB369A86E24C4185DB08	50404B08111323C691E1695737556E4AFCDCC87EADD22C5503B6D03392AADDDF	UCA Global G2 Root
8	UCA Global G2 Root	Signing Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	BB61408AED9F530B2EC0545E53BA2C8EBEAA57D9976447DB1663CED4600CD6B7	Certum Trusted Network CA
9	UCA Global G2 Root	Signing Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	BFA95C5DF164B659FA32F6D10564D7170DDE661A853A782E6AB63639433BCB41	Certum Trusted Network CA

Sub CAs

#	CA Name	Key Type	Signature Algorithm	Key Size	Subject DN	Subject Key Identifier	Certificates Thumbprint (SHA256)	Certificate Signed by
10i	SHECA IV SMIME RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA IV SMIME RSA CA 1A O = UniTrust C = CN	0731D082BC0A0AEF2F464617AF73F5C05E3976BE	82BA6F1067468383757DF53F1628258043BBB972E1CAD31FD7AAD0ADD66A5B53	UniTrust Global SMIME RSA Root CA R1
11	SHECA MV SMIME RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA MV SMIME RSA CA 1A O = UniTrust C = CN	838975C497C317A6532B73F31C7FBCAEA2FE1E90	92148A115D26B287254B36164164B2220EE36B405D3B708CF5B7AB060C66B1FE	UniTrust Global SMIME RSA Root CA R1
12	SHECA OV SMIME RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA OV SMIME RSA CA 1A O = UniTrust C = CN	82964C637D30CB2841C53AC7E84D1EB99489FF5A	6B661B964F2359C4CA68355243A2EEEDA9BACDA191D103A0C1119EC892018AC7	UniTrust Global SMIME RSA Root CA R1
13	SHECA IV SMIME ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA IV SMIME ECC CA 2A O = UniTrust C = CN	983BC3F8CEA554065FB1CD3F99F4B76AB2C22EC5	E82D794C1AC79F9BEBF3B6D98A237F84C15FD40C3ABB86C2214E699414F8FF54	UniTrust Global SMIME ECC Root CA R2
14	SHECA MV SMIME ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA MV SMIME ECC CA 2A O = UniTrust C = CN	D9B98D06C0DBD56A3497D7A9B0E9AE8B61B9F032	D7C4AB9D315AE8B889DA902C55264295D8CDC0F5471370490F4D4585E2C3C6D3	UniTrust Global SMIME ECC Root CA R2
15	SHECA OV SMIME ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA OV SMIME ECC CA 2A O = UniTrust C = CN	1CD15D6061277F084A21AD9518E43191D639DC18	229B7FBCA2361DE63171067DE91DFFB3D2FA71A5ABE51CA41D5300C5750D2F0E	UniTrust Global SMIME ECC Root CA R2

#	CA Name	Key Type	Signature Algorithm	Key Size	Subject DN	Subject Key Identifier	Certificates Thumbprint (SHA256)	Certificate Signed by
16	SHECA SMIME CA G1	Signing Key	sha256RSA	2048 bits	CN = SHECA SMIME CA G1 O = UniTrust C = CN	1FA80B4DCF9CA6A53ADAB096AB9957B90A9B7F5D	8100D384D6C4529883C37C37C68FD4903C41CCBCB9033A9C733A6AF0806E1DE7	UCA Global G2 Root
17	SHECA MV SMIME RSA CA G1	Signing Key	sha384RSA	3072 bits	CN = SHECA MV SMIME RSA CA G1 O = UniTrust C = CN	4F111E8FD4506500D7CE565190AF012BFB143845	C064FAB74E8723164932A25CFB6708106E1E5A3A05CFD1079B1DCF52792C5908	UCA Global G2 Root
18	SHECA IV SMIME RSA CA G1	Signing Key	sha384RSA	3072 bits	CN = SHECA IV SMIME RSA CA G1 O = UniTrust C = CN	E010A54E644A8F605F134C5C108E742C0168BBE5	2A1AAA3E4D7C6EC8BE083BDBDD247153A88D51F1226FD9691B872AE23D166BFF	UCA Global G2 Root
19	SHECA OV SMIME RSA CA G1	Signing Key	sha384RSA	3072 bits	CN = SHECA OV SMIME RSA CA G1 O = UniTrust C = CN	E3B8865D1EF2FF2146219648BD54022EC93BC85C	73BA9F7AE0924F3567F0280568A7050A58C9C4855DE0686C2FDC48522EB86D2D	UCA Global G2 Root

Attachment B

The list of SHECA's Certification Practice Statements covered in the management's assertion for the period from April 1, 2025 to March 31, 2026 is as follow:

Policy Name	Version
UniTrust Certification Practice Statement	V3.8.2
	V3.8.1
	V3.8.0
	V3.7.9
UniTrust Certificate Policy	V1.6
	V1.5.9
	V1.5.8
	V1.5.7
SHECA SMIME CP/CPS	V1.1
	V1.0