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

- disclosed its extended validation TLS ("EV TLS") certificate lifecycle management business practices in its Certificate Policies/Certification Practice Statements ("CP"/ "CPS") enumerated in Attachment B, including its commitment to provide EV TLS certificates in conformity with the CA/Browser Forum Requirement 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 EV TLS certificates it manages is established and protected throughout their lifecycles; and

  - EV TLS subscriber information is properly authenticated (for the registration activities performed by SHECA),

in accordance with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation TLS v2.0.1.

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 – Extended Validation TLS v2.0.1.

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 – Extended Validation TLS v2.0.1. 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 EV TLS certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of EV TLS certificates; (2) selectively testing transactions executed in accordance with disclosed EV TLS 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 – Extended Validation TLS v2.0.1.

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 – Extended Validation TLS v2.0.1, nor the suitability of any of SHECA's services for any customer's intended purpose. Our opinion is not modified in respect of this matter.

Other Matter

SHECA's management has disclosed 2 incidents (see Attachment C) during the period from April 1, 2025 to March 31, 2026. The remedial actions and the root causes of these incidents undertaken by SHECA have been posted publicly in the online forums of the Bugzilla site, as well as the online forums of individual internet browsers that comprise the CA/Browser Forum.

Our opinion is not modified in respect of 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 – Extended Validation TLS v2.0.1 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 t the WebTrust Principles and Criteria for Certification Authorities – Extended Validation TLS v2.0.1.

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 – Extended Validation TLS 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 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
2	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
3	UniTrust Global TLS RSA Root CA R1	Root Key	sha384RSA	4096 bits	CN = UniTrust Global TLS RSA Root CA R1 O = UniTrust C = CN	E349C5A5003582FB630CBB369A86E24C4185DB08	4BABE0E9328D5DAE17936F3DDAA2442BFBDD0873F92FB8D1FBBD3D9894649AD9	UniTrust Global TLS RSA Root CA R1
4	UniTrust Global TLS ECC Root CA R2	Root Key	sha384ECDSA	384 bits	CN = UniTrust Global TLS ECC Root CA R2 O = UniTrust C = CN	46E3D4F8DF88838AB7AE69966E00526FBB43D791	6C689FC6B014A1FB0CDEB5A3996171C15E7286106028532E0210CEA8D9CD4E97	UniTrust Global TLS ECC Root CA R2
5	UCA Extended Validation Root	Root Key	sha256RSA	4096 bits	CN = UCA Extended Validation Root O = UniTrust C = CN	D9743AE4303D0DF712DC7E5A059F1E349AF7E114	D43AF9B35473755C9684FC06D7D8CB70EE5C28E773FB294EB41EE71722924D24	UCA Extended Validation Root
6	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
7	UniTrust Global TLS ECC Root CA R2	Signing Key	sha384RSA	384 bits	CN = UniTrust Global TLS ECC Root CA R2	46E3D4F8DF88838AB7AE69966E00526FBB43D791	8ED6FA47B14DC79C85ED5C4CE2C67B2F2F96D2B9054690F28BF2DFE9A5770DF0	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	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
9	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
10	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
11	UCA Global G2 Root	Signing Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	BB61408AED9F530B2EC0545E53BA2C8EBEAA57D9976447DB1663CED4600CD6B7	Certum Trusted Network CA
12	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
13	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
14	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
15	SHECA EV TLS RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA EV TLS RSA CA 1A O = UniTrust C = CN	405C000B86462082A0BFB2C60063410365662F04	B2525A5966CA68CA7F504F0A21FD73847D174F89B48852A3E970588E1EAFC774	UniTrust Global TLS RSA Root CA R1
16	SHECA EV TLS RSA CA 2026 S1	Signing Key	sha384RSA	3072 bits	CN = SHECA EV TLS RSA CA 2026 S1	197C4FE5F58C6BFD7EEB9AA02D1E78444CF1FFF7	B0CBFA69D8D4F658CF761C2B0CF73B84A90022EF5B977B13E06EC42B913DE1F1	UniTrust Global TLS RSA Root CA R1

#	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 EV TLS ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA EV TLS ECC CA 2A O = UniTrust C = CN	6DB05C0FE4066E45643147106EA3F20327D3ACBC	05E4C4B1F258030690E6793C9C13C6F6AE234F68E5C41236FDC919B7F589032F	UniTrust Global TLS ECC Root CA R2
18	SHECA EV TLS ECC CA 2026 S1	Signing Key	sha384ECDSA	384 bits	CN = SHECA EV TLS ECC CA 2026 S1 O = UniTrust C = CN	C1BAAF0B91C9D8C786E14C722B965CE2272E1B9D	2C0B55DF3E6F26B4133CD04AE7B7A62F1DCEFD4C27E7D73A30CB25D914786E98	UniTrust Global TLS ECC Root CA R2
19	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
20	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
21	SHECA EV TLS RSA CA C1	Signing Key	sha384RSA	3072 bits	CN = SHECA EV TLS RSA CA C1 O = UniTrust C = CN	8A4E9A2D57D50731375FE5B8510789630B804877	15F4F5D5A8D6DED4CDD54CE4E1B367203B7F2CDF416104BA5D6405AF55AC8045	UCA Extended Validation Root
22	SHECA EV TLS ECC CA C2	Signing Key	sha384RSA	384 bits	CN = SHECA EV TLS ECC CA C2 O = UniTrust C = CN	AEAFD7E1680007D1875357883EDDF298E3C8983C	E3BF9CA7BC56D03EE6BAE52E3FBA47CAFE4198F2A026C8278087D82B951E428C	UCA Extended Validation Root
23	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

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 EV Certification Practice Statement	V1.5.9
	V1.5.8
	V1.5.7
UniTrust EV Certificate Policy	V1.7.5
	V1.7.4
	V1.7.3
SHECA TLS CP/CPS	V1.4
	V1.3
	V1.2
	V1.1
	V1.0

Attachment C

SHECA's management has disclosed 2 incidents during the period from April 1, 2025 to March 31, 2026. We perform procedures to understand the root cause disclosed by SHECA, and if facts and circumstances noted in our examination agreed with what has been disclosed. We have also considered the procedures SHECA has designed and noted if implemented properly and operated effectively, the controls would address the root cause. We did not perform any procedures subsequent to this report as to the effectiveness of the controls implemented. The list of incidents disclosed publicly during the period from April 1, 2025 to March 31, 2026 is as follow:

Bugzilla ID	Description	Status	Related to WebTrust requirements	Related to industry requirements
#1946921	SHECA: DV SSL certificate format is abnormal	Closed	Yes	Yes
#1981380	SHECA: Issuing with OV Policy OID but not an OV cert, duplicate of #1946921	Closed	Yes	Yes

Attachment D

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), and provides Extended Validation TLS ("EV TLS") CA services.

The management of SHECA is responsible for establishing and maintaining effective controls over its EV TLS CA operations, including its EV TLS CA business practices disclosure on its website, EV TLS key lifecycle management controls, and EV TLS 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 EV TLS CA services. Based on that assessment, in SHECA management's opinion, in providing its EV TLS Certification Authority (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 extended validation TLS ("EV TLS") certificate lifecycle management business practices in its Certificate Policies/Certification Practice Statements ("CP"/ "CPS") enumerated in Attachment B, including its commitment to provide EV TLS certificates in conformity with the CA/Browser Forum Guidelines 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 EV TLS certificates it manages is established and

protected throughout their lifecycles; and

- EV TLS subscriber information is properly authenticated (for the registration activities performed by SHECA)

in accordance with the WebTrust Principles and Criteria for Certification Authorities - Extended Validation TLS v2.0.1.

SHECA has disclosed 2 incidents (see Attachment C) during the period from April 1, 2025 to March 31, 2026. 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.

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 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
2	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
3	UniTrust Global TLS RSA Root CA R1	Root Key	sha384RSA	4096 bits	CN = UniTrust Global TLS RSA Root CA R1 O = UniTrust C = CN	E349C5A5003582FB630CBB369A86E24C4185DB08	4BABE0E9328D5DAE17936F3DDAA2442BFBDD0873F92FB8D1FBBD3D9894649AD9	UniTrust Global TLS RSA Root CA R1
4	UniTrust Global TLS ECC Root CA R2	Root Key	sha384ECDSA	384 bits	CN = UniTrust Global TLS ECC Root CA R2 O = UniTrust C = CN	46E3D4F8DF88838AB7AE69966E00526FBB43D791	6C689FC6B014A1FB0CDEB5A3996171C15E728610602853 2E0210CEA8D9CD4E97	UniTrust Global TLS ECC Root CA R2
5	UCA Extended Validation Root	Root Key	sha256RSA	4096 bits	CN = UCA Extended Validation Root O = UniTrust C = CN	D9743AE4303D0DF712DC7E5A059F1E349AF7E114	D43AF9B35473755C9684FC06D7D8CB70EE5C28E773FB294EB41EE71722924D24	UCA Extended Validation Root
6	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
7	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
8	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
9	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
10	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
11	UCA Global G2 Root	Signing Key	sha256RSA	4096 bits	CN = UCA Global G2 Root O = UniTrust C = CN	81C48CCCF5E430FFA50C085F8C1567217401DFDF	BB61408AED9F530B2EC0545E53BA2C8EBEAA57D9976447DB1663CED4600CD6B7	Certum Trusted Network CA
12	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
13	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
14	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

#	CA Name	Key Type	Signature Algorithm	Key Size	Subject DN	Subject Key Identifier	Certificates Thumbprint (SHA256)	Certificate Signed by
15	SHECA EV TLS RSA CA 1A	Signing Key	sha384RSA	3072 bits	CN = SHECA EV TLS RSA CA 1A O = UniTrust C = CN	405C000B8646208265662F04	B2525A5966CA68CA7F504F0A21FD73847D174F89B48852A3E970588E1EAFC774	UniTrust Global TLS RSA Root CA R1
16	SHECA EV TLS RSA CA 2026 S1	Signing Key	sha384RSA	3072 bits	CN = SHECA EV TLS RSA CA 2026 S1 O = UniTrust C = CN	197C4FE5F58C6BFD7EEB9AA02D1E78444CF1FFF7	B0CBFA69D8D4F658CF761C2B0CF73B84A90022EF5B977B13E06EC42B913DE1F1	UniTrust Global TLS RSA Root CA R1
17	SHECA EV TLS ECC CA 2A	Signing Key	sha384ECDSA	384 bits	CN = SHECA EV TLS ECC CA 2A O = UniTrust C = CN	6DB05C0FE4066E45643147106EA3F20327D3ACBC	05E4C4B1F258030690E6793C9C13C6F6AE234F68E5C41236FDC919B7F589032F	UniTrust Global TLS ECC Root CA R2
18	SHECA EV TLS ECC CA 2026 S1	Signing Key	sha384ECDSA	384 bits	CN = SHECA EV TLS ECC CA 2026 S1 O = UniTrust C = CN	C1BAAF0B91C9D8C786E14C722B965CE2272E1B9D	2C0B55DF3E6F26B4133CD04AE7B7A62F1DCEFD4C27E7D73A30CB25D914786E98	UniTrust Global TLS ECC Root CA R2
19	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
20	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
21	SHECA EV TLS RSA CA C1	Signing Key	sha384RSA	3072 bits	CN = SHECA EV TLS RSA CA C1 O = UniTrust C = CN	8A4E9A2D57D50731375FE5B8510789630B804877	15F4F5D5A8D6DED4CDD54CE4E1B367203B7F2CDF416104BA5D6405AF55AC8045	UCA Extended Validation Root
22	SHECA EV TLS ECC CA C2	Signing Key	sha384RSA	384 bits	CN = SHECA EV TLS ECC CA C2 O = UniTrust C = CN	AEAFD7E1680007D1875357883EDDF298E3C8983C	E3BF9CA7BC56D03EE6BAE52E3FBA47CAFE4198F2A026C8278087D82B951E428C	UCA Extended Validation Root
23	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

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 EV Certification Practice Statement	V1.5.9
	V1.5.8
	V1.5.7
UniTrust EV Certificate Policy	V1.7.5
	V1.7.4
	V1.7.3
SHECA TLS CP/CPS	V1.4
	V1.3
	V1.2
	V1.1
	V1.0

Attachment C

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

Bugzilla ID	Description	Status	Related to WebTrust requirements	Related to industry requirements
#1946921	SHECA: DV SSL certificate format is abnormal	Closed	Yes	Yes
#1981380	SHECA: Issuing with OV Policy OID but not an OV cert, duplicate of #1946921	Closed	Yes	Yes