

INDEPENDENT ASSURANCE REPORT

To the management of TrustAsia Technologies, Inc. ("TrustAsia"):

We have been engaged, in a reasonable assurance engagement, to report on TrustAsia management's assertion that for its Certification Authority (CA) operations at locations as enumerated in Appendix C, throughout the period 1 August 2023 to 31 July 2024 for its CAs as enumerated in Appendix A, TrustAsia has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its Certification Practice Statement (CPS) and Certificate Policy (CP) as enumerated in Appendix B
- maintained effective controls to provide reasonable assurance that:
 - TrustAsia's Certification Practice Statement is consistent with its Certificate Policy
 - TrustAsia provides its services in accordance with its Certificate Policy and Certification Practice Statement
- 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; and
 - subscriber information is properly authenticated
- 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](#).

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

After the planned new site within the same city as the main datacenter went into operations during the audit period, TrustAsia had relocated its system resources for production operations from the original data center at Shanghai (East) to the new site at Shanghai (West) and transported all key materials from the original main site to the new site as the new secure location hosting the key materials within the scope. Corresponding controls had been examined for existence and effectiveness physically on site before the new site went into operations and migration conducted for readiness and compliance.

Certification authority's responsibilities

TrustAsia's management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with the [WebTrust Principles and Criteria for Certification Authorities, v2.2.2](#).

Our independence and quality control

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* 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.

The firm applies International Standard on Quality Management (ISQM) 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements* and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Auditor's responsibilities

Our responsibility is to express an opinion on management's assertion based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's assertion is fairly stated, and, accordingly, included:

- (1) obtaining an understanding of TrustAsia'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.

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

Relative effectiveness of controls

The relative effectiveness and significance of specific controls at TrustAsia 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.

Inherent limitations

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

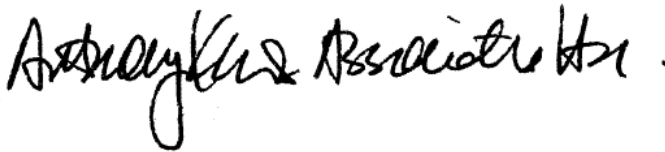
Opinion

In our opinion, throughout the period 1 August 2023 to 31 July 2024, TrustAsia management's assertion, as referred to above, is fairly stated, in all material respects, in accordance with the [WebTrust Principles and Criteria for Certification Authorities, v2.2.2](#).

This report does not include any representation as to the quality of TrustAsia's services beyond those covered by the [WebTrust Principles and Criteria for Certification Authorities, v2.2.2](#), nor the suitability of any of TrustAsia's services for any customer's intended purpose.

Use of the WebTrust seal

TrustAsia'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.



Anthony Kam & Associates Ltd.

Certified Public Accountants

2105 Wing On Ctr, 111 Connaught Road, HK SAR, China

14 Oct 2024

KAM Hau Choi Anthony

Practising Certificate Number P02558

Appendix A

The list of keys and certificates covered in the report is as follow:

Subject DN	Key Type	Signature Algorithm	Key Size	Subject Key Identifier	SHA256 Certificate Thumbprints	Certificate Signed by
CN = TrustAsia Global Root CA G1 O = TrustAsia Technologies, Inc. C = CN	Root Key	Sha256RSA	4096 bits	24C20F2CCDC 0B5154F6B6D D4F2F058FE1 443DFF4	05F82DE4B4 A9ED4B7CD1 F3ACE9B73B D6DB69D878 16DD384719 5CF737ED29 51E7	TrustAsia Global Root CA G1
CN = TrustAsia DV TLS RSA CA O = TrustAsia Technologies, Inc. C = CN	Signing Key	Sha256RSA	4096 bits	BF3FDED0466 D4A50CFE2FB E20B854834C 1AFB825	322C1AFDCC 9827AC4D23 4780082A98 6203494199 8AFF67E6D7 7BC4C560DB 25B4	TrustAsia Global Root CA G1
CN = TrustAsia OV TLS RSA CA O = TrustAsia Technologies, Inc. C = CN	Signing Key	Sha256RSA	4096 bits	EFD7A5E0375 A8E6A5D60CF BBDDFE80F23 83985EA	624FD02328 D23289573E BA7D184525 8D70E15BC2 81E7DA38DC E06A5712B2 54A1	TrustAsia Global Root CA G1
CN = TrustAsia EV TLS RSA CA O = TrustAsia Technologies, Inc. C = CN	Signing Key	Sha256RSA	4096 bits	9C95683DD43 AC03DD2BA2B AC315C4CAD5 3BC90CD	853B06C42E 26160305CC 3DD5B1F7F7 DC6BAC5602 C0F444F08D 45A7DEE1F4 7CF8	TrustAsia Global Root CA G1
CN = TrustAsia Code Signing RSA CA O = TrustAsia Technologies, Inc. C = CN	Signing Key	Sha256RSA	4096 bits	F1ECAAF24AAA EE1F2958F17 2AB838B9F86 FC394B9	4A14A381B9 F2E7A7A49E FA3A87360D B433C6DAF7 B80E06F675 72EA892437 5B60	TrustAsia Global Root CA G1
CN = TrustAsia EV Code Signing RSA CA O = TrustAsia Technologies, Inc. C = CN	Signing Key	Sha256RSA	4096 bits	4B2572DF664 CBD56C3F9FB ED36BC287E2 9AE0326	982222E6B2 485A0A80C1 7209630EA9 749B8785E6 C75D6475B3 E4AA578D90 1DF5	TrustAsia Global Root CA G1
CN = TrustAsia Document Signing RSA CA O = TrustAsia Technologies, Inc. C = CN	Signing Key	Sha256RSA	4096 bits	68752DEB635 AC881EFC268 430CF215C55 64D63E5	033C44B6C7 11CA26E7B5 ABFD36B721 10F5944146 D99E92C020 266B90FDD7 66A6	TrustAsia Global Root CA G1

CN = TrustAsia Secure Email RSA CA O = TrustAsia Technologies, Inc. C = CN	Signing Key	Sha256RSA	4096 bits	FCB3E33D448 455D2FF172D 1C4DF961090 3C6D94A	E67767E9C72 E0691497F66 616590D99AF DC60974FE6F 1F4F1BFD71B 2A13E2C03	TrustAsia Global Root CA G1
CN = TrustAsia TimeStamping RSA CA O = TrustAsia Technologies, Inc. C = CN	Signing Key	Sha256RSA	4096 bits	7F0BBE8BB42 329F2811B0A 538415ABCE6 27E5BD8	748F6BD8667 C2158C3E384 27D9039BE0B C4C016EF0BE EB73B8BDF0 42B343974	TrustAsia Global Root CA G1
CN = TrustAsia Global Root CA G2 O = TrustAsia Technologies, Inc. C = CN	Root Key	sha384ECDSA	384 bits	4FEB2996F4F 142DE5AA207 56B2FF59C28 53EC398	1DF7E8B185C A46578D458D 05129854FDE 32EF1E9B36F 0B96963CE38 CAEABE4BC	TrustAsia Global Root CA G2
CN = TrustAsia DV TLS ECC CA O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	C12D72D0E89 25B196052C0 DCEE6A734D2 1191706	C3D06E52712 33ED46A538C 150FDCDCD73 F88AECEFE24 B8D16F981C1 3742E924D	TrustAsia Global Root CA G2
CN = TrustAsia OV TLS ECC CA O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	F3118C08803 CE2E7D69301 9F7D422BAC7 B4DE39F	5655EAAF713 3936558CADD E8F3447615F 759C9C63BEE 949D4DC3CD7 FB71FCBED	TrustAsia Global Root CA G2
CN = TrustAsia EV TLS ECC CA O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	1C72953489D 756FE3D84BD AD33B51C1DD 9472536	2126C130F1D 576FB70CF3B 8E8C0EA2FEE 8CFE98D7213 04EAAA6D898 E721029CE	TrustAsia Global Root CA G2
CN = TrustAsia Global Root CA G3 O = TrustAsia Technologies, Inc. C = CN	Root Key	sha384RSA	4096 bits	40E4E4F223E F38CAB0AE57 7FF22130163 4DBBC92	E0D3226AEB 1163C2E48F F9BE3B50B4 C6431BE7BB 1EACC5C36B 5D5EC50903 9A08	TrustAsia Global Root CA G3
CN = TrustAsia DV TLS RSA CA G3 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	FFD38BE629C 8A6994DE519 6BF8FFAF394 19D7ED6	E0DD6743D6 D08E2AB188 84ED1E7E46 B3D9726FFF A9B1866642 AEBF266FDA 2654	TrustAsia Global Root CA G3

CN = TrustAsia OV TLS RSA CA G3 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	22AADBB42F7 F3C183F717E CD61FD4ECE4 656EF54	573F5F7974 82F567EDC7 901879457B C46C9DF0AC FD8CE7B1A8 FB7E2218FA 477B	TrustAsia Global Root CA G3
CN = TrustAsia EV TLS RSA CA G3 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	22C292A6316 3AC13C7176A 4F313B25727 37CD26A	15DDF98C57 E0F46E5C5E E00283BC4A F8FE0E8D2C 42151630DE FFFA285EA6 2D09	TrustAsia Global Root CA G3
CN = TrustAsia Code Signing RSA CA G3 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	A3ED9A5FE3D FE8CE6AB41E C63C625FDCA C9A0682	FA012B12A4 53DAF7C02B D7F8FF617A 4C91EB2953 D3E42F6FDB 000EAE4FB6 FAAE	TrustAsia Global Root CA G3
CN = TrustAsia EV Code Signing RSA CA G3 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	217C9E5F581 AC037C9EEAC CADA99DB861 393B1C3	DD169948C5 6F90D640E3 92F7A69452 EC4B394E6A D179FF54F7 E7DBB6AACF BDBA	TrustAsia Global Root CA G3
CN = TrustAsia Document Signing RSA CA G3 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	0521A508833 75645B4055F 1B6D206127D 85E8143	B7DE90291B 7905CBDB8C 744E98F1E6 FC97C2288B 2177F79D91 6D18D31AE8 B2A7	TrustAsia Global Root CA G3
CN = TrustAsia Secure Email RSA CA G3 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	EB164C7D748 A091C5787C3 5B9B98FF213 6C3B20A	C84E9EE5225 DF7B674A573 43C6D489219 07E97640100 42E40B2C00F 944639CA4	TrustAsia Global Root CA G3
CN = TrustAsia TimeStamping RSA CA G3 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	8BEE09E649C 638F4A45176 DBAE1B1013A F231775	904A794C751 20499475947 46743265348 A339A7573E2 323B9D4BE89 BBAFA5D52	TrustAsia Global Root CA G3
CN = TrustAsia Global Root CA G4 O = TrustAsia Technologies, Inc. C = CN	Root Key	sha384ECDSA	384 bits	A5BB4A97CEB 32B7FA431DE 97835983A66 F71CBDE	BE4B56CB505 6C0136A526D F444508DAA3 6A0B54F42E4 AC38F72AF47 0E479654C	TrustAsia Global Root CA G4
CN = TrustAsia DV TLS ECC CA G4 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	0C09D741BDF 04CB767E4B0 56BF7E8DB91 433322F	C28348740DA 36CF14DDC49 280CF030AB9 CE3B0ACE093 B0E1BA18945 6F4918B9C	TrustAsia Global Root CA G4

CN = TrustAsia OV TLS ECC CA G4 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	76533221F36 F769D585329 33BEF548B9E 2284FEF	EEE6BAF50B1 4BCA04202B4 96737E676F7 13E7431FFD4 FCA1309F661 481EC520F	TrustAsia Global Root CA G4
CN = TrustAsia EV TLS ECC CA G4 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	EF46439CE9F 4121DF11A18 1968571D84B AAF7D19	C261EE3D4BB DC456FFB678 68363FED80C B5C9AD7AF3F 5A5DACBE32B ECDD88A7	TrustAsia Global Root CA G4
CN = TrustAsia Code Signing ECC CA G4 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	FB7514C9DD3 5A7003A3C13 54259BFDD3 F02DCF6	933ECE2B4EB B0557072C7B 408F6D36A54 0524C3D1A60 F260C97D962 9D060BA7B	TrustAsia Global Root CA G4
CN = TrustAsia EV Code Signing ECC CA G4 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	C722B5F7C34 ADC9B2C1958 5BC16672266 36CF4E3	6A423235B3B 26C7DED5359 BF0BAD4EE30 1729DAF8287 244FC9995B0 605268EDB	TrustAsia Global Root CA G4
CN = TrustAsia Document Signing ECC CA G4 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	DEA970A22DB 35572EB5849 77653F23479 C4F74A1	84598841793 B351DD3AD8C 11A521CAD00 270CF64663C 80002A02557 2F8020792	TrustAsia Global Root CA G4
CN = TrustAsia Secure Email ECC CA G4 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	613250574BF 3266AE9C8D7 C61337F17E1 553B3AC	70342F6C5E0 FD9F9ABE3C1 448D033E1A0 CAB4CC56040 9E1C03B626E 48B8B16DD	TrustAsia Global Root CA G4
CN = TrustAsia TimeStamping ECC CA G4 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	6CDF8F267CE 820FE629B3F A81F15EEEE7 CF54C46	B917AB79332 B73B9386552 89C287F183E 55B1BC60873 845ABA119DB 93D2E3C08	TrustAsia Global Root CA G4
CN = TrustAsia TLS RSA Root CA O = TrustAsia Technologies, Inc. C = CN	Root Key	sha384RSA	4096 bits	B80791795C0 6F446FD7B59 CA5A2691A74 52BF853	06C08D7DAFD 876971EB112 4FE67F847EC 0C7A158D3EA 53CBE940E2E A9791F4C3	TrustAsia TLS RSA Root CA

CN = TrustAsia DV TLS RSA CA 2024 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	6175054E1AF50FC1602020C228D98BB3E2C17DB4	5EB0217B928C2DE1170FCE110CACC3C89A42492E4F97F5AE1EB8CD54F8A68EEB	TrustAsia TLS RSA Root CA
CN = TrustAsia OV TLS RSA CA 2024 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	967C1342724B3A936C501AEDEE18113A9F9C250D	D0B626C8AD93962296B3920106ED7FB3818FCB98E0B73E799141B42521335B0F	TrustAsia TLS RSA Root CA
CN = TrustAsia EV TLS RSA CA 2024 V2 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	5B1A314630DC3325DD98258EEF84D189CA4BB826	D886C235FAFADD2E4734924CF58B4D8F0CB7065F0F5451B3E1C308F92EF7B2EB	TrustAsia TLS RSA Root CA
CN = TrustAsia TLS ECC Root CA O = TrustAsia Technologies, Inc. C = CN	Root Key	sha384ECDSA	384 bits	2C8553BBB143CD32EA9EA387FEA298A8A693E910	C0076B9EF0531FB1A656D67C4EBE97CD5DBAA41EF44598ACC2489878C92D8711	TrustAsia TLS ECC Root CA
CN = TrustAsia DV TLS ECC CA 2024 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	D0B70CEDFC5402C2C05D7E3B17EBBF1050B19665	73E9BE7D57BD5C72A06304463D32F8F85ECA12E2F2D284E48AE83F653FDB4EB6	TrustAsia TLS ECC Root CA
CN = TrustAsia OV TLS ECC CA 2024 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	A4534BA525BAAA848E0B879DC94EAA3ADD0EBAC6	0E975E62A83030EAE3F441BAFFBFD7574FB7235EECB50F1F747DF8F0506D245E	TrustAsia TLS ECC Root CA
CN = TrustAsia EV TLS ECC CA 2024 V2 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	8E8ECB35F18158AA202DCEC336168A10113859C7	D19E1FCD8E12747D75B74A28318EEFDD700F616E2B215701BBE804C3CDDA027B	TrustAsia TLS ECC Root CA
CN = TrustAsia CS RSA Root CA O = TrustAsia Technologies, Inc. C = CN	Root Key	sha384RSA	4096 bits	B12E11466A82339CD3F2F018529A607B792A79E	F38AB64B30C0D900B7212A793651B87F287C575224007F3B8851618FD5B48DEB	TrustAsia CS RSA Root CA

CN = TrustAsia CS RSA CA 2024 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	7EB2529B31F 4F4B4F7D5BE 0F831028CD6 8C08AAE	0C67D64F643 0F927EB3772 677ADFC5C23 6A14E3DF7A7 66BFF299FB7 EAB1EF315	TrustAsia CS RSA Root CA
CN = TrustAsia CS ECC Root CA O = TrustAsia Technologies, Inc. C = CN	Root Key	sha384ECDSA	384 bits	5D875EB48E9 6795EB534A5 42B1C3798F7 35DEF4B	6B9C91E5A64 53375EF905D 8F2A5369953 065F471664F 2E676E2013D F388C9B56	TrustAsia CS ECC Root CA
CN = TrustAsia CS ECC CA 2024 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	708C1FD8C6B 1AA07387BA7 8F3BAA23039 9AE53C1	5CF4B9BC8D9 BA4A96DE8BC 3B5C38D0372 B0A0187DD1A 9AE985647A8 1F077610B	TrustAsia CS ECC Root CA
CN = TrustAsia SMIME RSA Root CA O = TrustAsia Technologies, Inc. C = CN	Root Key	sha384RSA	4096 bits	801AAA43C1C 97F8B1A9645 BC3DBB6B485 26C5BAB	C7796BEB62C 101BB143D26 2A7C96A0C61 68183223EF5 0D699632D86 E03B8CC9B	TrustAsia SMIME RSA Root CA
CN = TrustAsia SMIME RSA CA 2024 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	20741B3D532 5D2968E2846 8167E43DB50 550784B	BC2197C0C1F F17C553370B F9955B9B50C 8C9D27A0C28 F78704E00C8 81F1458AA	TrustAsia SMIME RSA Root CA
CN = TrustAsia SMIME ECC Root CA O = TrustAsia Technologies, Inc. C = CN	Root Key	sha384ECDSA	384 bits	3167E672B20 DE622A0ACCF 7E22A75932E 36623A5	436472C1009 A325C54F1A5 BBB5468A7BA EECCBE05DE5 F099CB70D3F E41E13C16	TrustAsia SMIME ECC Root CA
CN = TrustAsia SMIME ECC CA 2024 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	E1B057357F7 E7E7FC8B108 D39AA6D1F95 1EB9AA3	E21C0762F0B 1777AB2B06E 9F9273BE251 AB9FBB3D5DD 901F60750EF 9B53B8488	TrustAsia SMIME ECC Root CA
CN = TrustAsia TSA RSA Root CA O = TrustAsia Technologies, Inc. C = CN	Root Key	sha384RSA	4096 bits	38DC7012944 4CD6C205E3F D26AE5A4B3F 9EFAFA0	1498BFED947 C795235D348 2FBE493CD89 BE5DC074729 1C716360356 E89D4595E	TrustAsia TSA RSA Root CA

CN = TrustAsia TSA RSA CA 2024 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	81F63777034 F1EB469416D FFA4BB363AE E24E131	6AC8AF44575 A99945D01DD 0BD67527724 2D7DD1A515A 84D68E530EC 5000363C6	TrustAsia TSA RSA Root CA
CN = TrustAsia TSA ECC Root CA O = TrustAsia Technologies, Inc. C = CN	Root Key	sha384ECDSA	384 bits	25A66C22F38 0042663336C FD25A41E473 4FDFB6E	2E04BF6C4C9 1864389F7CB 30AFF4B5434 6794EF897B0 D6557F10B7A 8BA6D932C	TrustAsia TSA ECC Root CA
CN = TrustAsia TSA ECC CA 2024 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	D080C71A271 6F07AFC00D4 50A1AAC5F22 FB3179D	03053C0713B 9543C40B233 1FF5B571270 DF729B41087 DF450BCE44F 455AB8158	TrustAsia TSA ECC Root CA

Appendix B

Applicable versions of Certification Practice Statement (CPS) and Certificate Policy (CP) in-scope:

Name	Version	Date
TrustAsia Certificate Policy and Certification Practice Statement for Global Trusted Service	2.0	23 July 2024
TrustAsia Certificate Policy and Certification Practice Statement for Global Trusted Service	1.7.2	25 April 2024
TrustAsia Certificate Policy and Certification Practice Statement for Global Trusted Service	1.7.1	21 December 2023
TrustAsia Certificate Policy and Certification Practice Statement for Global Trusted Service	1.7.0	30 August 2023
TrustAsia Certificate Policy and Certification Practice Statement for Global Trusted Service	1.6.1	10 February 2023

Appendix C

Locations in-scope:

Location	Function
Shanghai (Central), China	Administration and Support
Shanghai (West), China	Datacenter Facility
Shanghai (East), China	Datacenter Facility

MANAGEMENT'S ASSERTION

TrustAsia Technologies, Inc. ("TrustAsia") operates the Certification Authority (CA) services known as CAs in Appendix A, and provides the following CA services:

- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation

The management of TrustAsia 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, and 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 TrustAsia's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

TrustAsia management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in TrustAsia management's opinion, in providing its Certification Authority (CA) services at locations as enumerated in Appendix C, throughout the period 1 August 2023 to 31 July 2024, TrustAsia has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its Certification Practice Statement (CPS) and Certificate Policy (CP) as enumerated in Appendix B
- maintained effective controls to provide reasonable assurance that:
 - TrustAsia's applicable versions of Certification Practice Statement are consistent with its applicable versions of Certificate Policy; and
 - TrustAsia provides its services in accordance with its Certificate Policy and Certification Practice Statement
- 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; and
 - subscriber information is properly authenticated
- maintained effective controls to provide reasonable assurance that:

- logical and physical access to CA systems and data is restricted to authorised individuals;
- the continuity of key and certificate management operations is maintained; and
- CA systems development, maintenance, and operations are properly authorised 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 and Maintenance
- Business Continuity Management
- Monitoring and Compliance
- Audit Logging

CA Key Lifecycle Management Controls

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

Certificate Lifecycle Management Controls

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

TrustAsia 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.

After the planned new site within the same city as the main datacenter went into operations during the audit period, TrustAsia had relocated its system resources for production operations from the original data center at Shanghai (East) to the new site at Shanghai (West) and transported all key materials from the original main site to the new site as the new secure location hosting the key materials within the scope. Corresponding controls had been examined for existence and effectiveness physically on site before the new site went into operations and migration conducted for readiness and compliance.



Mr. Xinyuan Zhai _____

CEO of TrustAsia Technologies, Inc.

32/ F, Building B, No.391, Gulping Road, Xuhui District, Shanghai, China

14 October 2024

Appendix A

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

Subject DN	Key Type	Signature Algorithm	Key Size	Subject Key Identifier	SHA256 Certificate Thumbprints	Certificate Signed by
CN = TrustAsia Global Root CA G1 O = TrustAsia Technologies, Inc. C = CN	Root Key	Sha256RSA	4096 bits	24C20F2CCDC0B5154F6B6D D4F2F058FE1443DFF4	05F82DE4B4A9ED4B7CD1 F3ACE9B73BD6B69D878 16DD3847195CF737ED29 51E7	TrustAsia Global Root CA G1
CN = TrustAsia DV TLS RSA CA O = TrustAsia Technologies, Inc. C = CN	Signing Key	Sha256RSA	4096 bits	BF3FDED0466D4A50CFE2FB E20B854834C1AFB825	322C1AFDCC9827AC4D23 4780082A986203494199 8AFF67E6D77BC4C560DB 25B4	TrustAsia Global Root CA G1
CN = TrustAsia OV TLS RSA CA O = TrustAsia Technologies, Inc. C = CN	Signing Key	Sha256RSA	4096 bits	EFD7A5E0375A8E6A5D60CF BBDDFE80F2383985EA	624FD02328D23289573E BA7D1845258D70E15BC2 81E7DA38DC E06A5712B2 54A1	TrustAsia Global Root CA G1
CN = TrustAsia EV TLS RSA CA O = TrustAsia Technologies, Inc. C = CN	Signing Key	Sha256RSA	4096 bits	9C95683DD43AC03DD2BA2B AC315C4CAD53BC90CD	853B06C42E26160305CC 3DD5B1F7F7DC6BAC5602 C0F444F08D45A7DEE1F4 7CF8	TrustAsia Global Root CA G1
CN = TrustAsia Code Signing RSA CA O = TrustAsia Technologies, Inc. C = CN	Signing Key	Sha256RSA	4096 bits	F1ECAFA24AAAE1F2958F17 2AB838B9F86FC394B9	4A14A381B9F2E7A7A49E FA3A87360DB433C6DAF7 B80E06F67572EA892437 5B60	TrustAsia Global Root CA G1
CN = TrustAsia EV Code Signing RSA CA O = TrustAsia Technologies, Inc. C = CN	Signing Key	Sha256RSA	4096 bits	4B2572DF664CBD56C3F9FB ED36BC287E29AE0326	982222E6B2485A0A80C1 7209630EA9749B8785E6 C75D6475B3E4AA578D90 1DF5	TrustAsia Global Root CA G1
CN = TrustAsia Document Signing RSA CA O = TrustAsia Technologies, Inc. C = CN	Signing Key	Sha256RSA	4096 bits	68752DEB635AC881EFC268 430CF215C5564D63E5	033C44B6C711CA26E7B5 ABFD36B72110F5944146 D99E92C020266B90FDD7 66A6	TrustAsia Global Root CA G1
CN = TrustAsia Secure Email RSA CA O = TrustAsia Technologies, Inc. C = CN	Signing Key	Sha256RSA	4096 bits	FCB3E33D448455D2FF172D 1C4DF9610903C6D94A	E67767E9C72E0691497F66 616590D99AFDC60974FE6F 1F4F1BFD71B2A13E2C03	TrustAsia Global Root CA G1

CN = TrustAsia TimeStamping RSA CA O = TrustAsia Technologies, Inc. C = CN	Signing Key	Sha256RSA	4096 bits	7F0BBE8BB42 329F2811B0A 538415ABCE6 27E5BD8	748F6BD8667 C2158C3E384 27D9039BE0B C4C016EF0BE EB73B8BDDFF0 42B343974	TrustAsia Global Root CA G1
CN = TrustAsia Global Root CA G2 O = TrustAsia Technologies, Inc. C = CN	Root Key	sha384ECDSA	384 bits	4FEB2996F4F 142DE5AA207 56B2FF59C28 53EC398	1DF7E8B185C A46578D458D 05129854FDE 32EF1E9B36F 0B96963CE38 CAEABE4BC	TrustAsia Global Root CA G2
CN = TrustAsia DV TLS ECC CA O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	C12D72D0E89 25B196052C0 DCEE6A734D2 1191706	C3D06E52712 33ED46A538C 150FDCDCD73 F88AECE624 B8D16F981C1 3742E924D	TrustAsia Global Root CA G2
CN = TrustAsia OV TLS ECC CA O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	F3118C08803 CE2E7D69301 9F7D422BAC7 B4DE39F	5655EAAF713 3936558CADD E8F3447615F 759C9C63BEE 949D4DC3CD7 FB71FCBED	TrustAsia Global Root CA G2
CN = TrustAsia EV TLS ECC CA O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	1C72953489D 756FE3D84BD AD33B51C1DD 9472536	2126C130F1D 576FB70CF3B 8E8C0EA2FEE 8CFE98D7213 04EAAA6D898 E721029CE	TrustAsia Global Root CA G2
CN = TrustAsia Global Root CA G3 O = TrustAsia Technologies, Inc. C = CN	Root Key	sha384RSA	4096 bits	40E4E4F223E F38CAB0AE57 7FF22130163 4DBBC92	E0D3226AEB 1163C2E48F F9BE3B50B4 C6431BE7BB 1EACC5C36B 5D5EC50903 9A08	TrustAsia Global Root CA G3
CN = TrustAsia DV TLS RSA CA G3 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	FFD38BE629C 8A6994DE519 6BF8FFAF394 19D7ED6	E0DD6743D6 D08E2AB188 84ED1E7E46 B3D9726FFF A9B1866642 AEBF266FDA 2654	TrustAsia Global Root CA G3
CN = TrustAsia OV TLS RSA CA G3 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	22AADB42F7 F3C183F717E CD61FD4ECE4 656EF54	573F5F7974 82F567EDC7 901879457B C46C9DF0AC FD8CE7B1A8 FB7E2218FA 477B	TrustAsia Global Root CA G3
CN = TrustAsia EV TLS RSA CA G3 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	22C292A6316 3AC13C7176A 4F313B25727 37CD26A	15DDF98C57 E0F46E5C5E E00283BC4A F8FE0E8D2C 42151630DE FFFA285EA6 2D09	TrustAsia Global Root CA G3

CN = TrustAsia Code Signing RSA CA G3 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	A3ED9A5FE3D FE8CE6AB41E C63C625FDCA C9A0682	FA012B12A4 53DAF7C02B D7F8FF617A 4C91EB2953 D3E42F6FDB 000EAE4FB6 FAAE	TrustAsia Global Root CA G3
CN = TrustAsia EV Code Signing RSA CA G3 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	217C9E5F581 AC037C9EEAC CADA99DB861 393B1C3	DD169948C5 6F90D640E3 92F7A69452 EC4B394E6A D179FF54F7 E7DBB6AACF BDBA	TrustAsia Global Root CA G3
CN = TrustAsia Document Signing RSA CA G3 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	0521A508833 75645B4055F 1B6D206127D 85E8143	B7DE90291B 7905CBDB8C 744E98F1E6 FC97C2288B 2177F79D91 6D18D31AE8 B2A7	TrustAsia Global Root CA G3
CN = TrustAsia Secure Email RSA CA G3 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	EB164C7D748 A091C5787C3 5B9B98FF213 6C3B20A	C84E9EE5225 DF7B674A573 43C6D489219 07E97640100 42E40B2C00F 944639CA4	TrustAsia Global Root CA G3
CN = TrustAsia TimeStamping RSA CA G3 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	8BEE09E649C 638F4A45176 DBAE1B1013A F231775	904A794C751 20499475947 46743265348 A339A7573E2 323B9D4BE89 BBAFA5D52	TrustAsia Global Root CA G3
CN = TrustAsia Global Root CA G4 O = TrustAsia Technologies, Inc. C = CN	Root Key	sha384ECDSA	384 bits	A5BB4A97CEB 32B7FA431DE 97835983A66 F71CBDE	BE4B56CB505 6C0136A526D F444508DAA3 6A0B54F42E4 AC38F72AF47 0E479654C	TrustAsia Global Root CA G4
CN = TrustAsia DV TLS ECC CA G4 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	0C09D741BDF 04CB767E4B0 56BF7E8DB91 433322F	C28348740DA 36CF14DDC49 280CF030AB9 CE3B0ACE093 B0E1BA18945 6F4918B9C	TrustAsia Global Root CA G4
CN = TrustAsia OV TLS ECC CA G4 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	76533221F36 F769D585329 33BEF548B9E 2284FEF	EEE6BAF50B1 4BCA04202B4 96737E676F7 13E7431FFD4 FCA1309F661 481EC520F	TrustAsia Global Root CA G4
CN = TrustAsia EV TLS ECC CA G4 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	EF46439CE9F 4121DF11A18 1968571D84B AAF7D19	C261EE3D4BB DC456FFB678 68363FED80C B5C9AD7AF3F 5A5DACBE32B ECDDDD88A7	TrustAsia Global Root CA G4

CN = TrustAsia Code Signing ECC CA G4 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	FB7514C9DD3 5A7003A3C13 54259BFDDE3 F02DCF6	933ECE2B4EB B0557072C7B 408F6D36A54 0524C3D1A60 F260C97D962 9D060BA7B	TrustAsia Global Root CA G4
CN = TrustAsia EV Code Signing ECC CA G4 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	C722B5F7C34 ADC9B2C1958 5BC16672266 36CF4E3	6A423235B3B 26C7DED5359 BF0BAD4EE30 1729DAF8287 244FC9995B0 605268EDB	TrustAsia Global Root CA G4
CN = TrustAsia Document Signing ECC CA G4 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	DEA970A22DB 35572EB5849 77653F23479 C4F74A1	84598841793 B351DD3AD8C 11A521CAD00 270CF64663C 80002A02557 2F8020792	TrustAsia Global Root CA G4
CN = TrustAsia Secure Email ECC CA G4 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	613250574BF 3266AE9C8D7 C61337F17E1 553B3AC	70342F6C5E0 FD9F9ABE3C1 448D033E1A0 CAB4CC56040 9E1C03B626E 48B8B16DD	TrustAsia Global Root CA G4
CN = TrustAsia TimeStamping ECC CA G4 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	6CDF8F267CE 820FE629B3F A81F15EEEA7 CF54C46	B917AB79332 B73B9386552 89C287F183E 55B1BC60873 845ABA119DB 93D2E3C08	TrustAsia Global Root CA G4
CN = TrustAsia TLS RSA Root CA O = TrustAsia Technologies, Inc. C = CN	Root Key	sha384RSA	4096 bits	B80791795C0 6F446FD7B59 CA5A2691A74 52BF853	06C08D7DAFD 876971EB112 4FE67F847EC 0C7A158D3EA 53CBE940E2E A9791F4C3	TrustAsia TLS RSA Root CA
CN = TrustAsia DV TLS RSA CA 2024 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	6175054E1AF 50FC1602020 C228D98BB3E 2C17DB4	5EB0217B928 C2DE1170FCE 110CACC3C89 A42492E4F97 F5AE1EB8CD5 4F8A68EEB	TrustAsia TLS RSA Root CA
CN = TrustAsia OV TLS RSA CA 2024 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	967C1342724 B3A936C501A EDEE18113A9 F9C250D	D0B626C8AD9 3962296B392 0106ED7FB38 18FCB98E0B7 3E799141B42 521335B0F	TrustAsia TLS RSA Root CA
CN = TrustAsia EV TLS RSA CA 2024 V2 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	5B1A314630D C3325DD9825 8EEF84D189C A4BB826	D886C235FAF ADD2E473492 4CF58B4D8F0 CB7065F0F54 51B3E1C308F 92EF7B2EB	TrustAsia TLS RSA Root CA

CN = TrustAsia TLS ECC Root CA O = TrustAsia Technologies, Inc. C = CN	Root Key	sha384ECDSA	384 bits	2C8553BBB14 3CD32EA9EA3 87FEA298A8A 693E910	C0076B9EF05 31FB1A656D6 7C4EBE97CD5 DBAA41EF445 98ACC248987 8C92D8711	TrustAsia TLS ECC Root CA
CN = TrustAsia DV TLS ECC CA 2024 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	D0B70CEDFC5 402C2C05D7E 3B17EBBF105 0B19665	73E9BE7D57B D5C72A06304 463D32F8F85 ECA12E2F2D2 84E48AE83F6 53FDB4EB6	TrustAsia TLS ECC Root CA
CN = TrustAsia OV TLS ECC CA 2024 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	A4534BA525B AAA848E0B87 9DC94EAA3AD D0EBAC6	0E975E62A83 030EAE3F441 BAFFBFD7574 FB7235EECB5 0F1F747DF8F 0506D245E	TrustAsia TLS ECC Root CA
CN = TrustAsia EV TLS ECC CA 2024 V2 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	8E8ECB35F18 158AA202DCE C336168A101 13859C7	D19E1FCD8E1 2747D75B74A 28318EEFDD7 00F616E2B21 5701BBE804C 3CDDA027B	TrustAsia TLS ECC Root CA
CN = TrustAsia CS RSA Root CA O = TrustAsia Technologies, Inc. C = CN	Root Key	sha384RSA	4096 bits	B12E11466A8 2339CD3F2F0 018529A607B 792A79E	F38AB64B30C 0D900B7212A 793651B87F2 87C57522400 7F3B8851618 FD5B48DEB	TrustAsia CS RSA Root CA
CN = TrustAsia CS RSA CA 2024 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	7EB2529B31F 4F4B4F7D5BE 0F831028CD6 8C08AAE	0C67D64F643 0F927EB3772 677ADFC5C23 6A14E3DF7A7 66BFF299FB7 EAB1EF315	TrustAsia CS RSA Root CA
CN = TrustAsia CS ECC Root CA O = TrustAsia Technologies, Inc. C = CN	Root Key	sha384ECDSA	384 bits	5D875EB48E9 6795EB534A5 42B1C3798F7 35DEF4B	6B9C91E5A64 53375EF905D 8F2A5369953 065F471664F 2E676E2013D F388C9B56	TrustAsia CS ECC Root CA
CN = TrustAsia CS ECC CA 2024 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	708C1FD8C6B 1AA07387BA7 8F3BAA23039 9AE53C1	5CF4B9BC8D9 BA4A96DE8BC 3B5C38D0372 B0A0187DD1A 9AE985647A8 1F077610B	TrustAsia CS ECC Root CA
CN = TrustAsia SMIME RSA Root CA O = TrustAsia Technologies, Inc. C = CN	Root Key	sha384RSA	4096 bits	801AAA43C1C 97F8B1A9645 BC3DDB6B485 26C5BAB	C7796BEB62C 101BB143D26 2A7C96A0C61 68183223EF5 0D699632D86 E03B8CC9B	TrustAsia SMIME RSA Root CA

CN = TrustAsia SMIME RSA CA 2024 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	20741B3D532 5D2968E2846 8167E43DB50 550784B	BC2197C0C1F F17C553370B F9955B9B50C 8C9D27A0C28 F78704E00C8 81F1458AA	TrustAsia SMIME RSA Root CA
CN = TrustAsia SMIME ECC Root CA O = TrustAsia Technologies, Inc. C = CN	Root Key	sha384ECDSA	384 bits	3167E672B20 DE622A0ACCF 7E22A75932E 36623A5	436472C1009 A325C54F1A5 BBB5468A7BA EECCBE05DE5 F099CB70D3F E41E13C16	TrustAsia SMIME ECC Root CA
CN = TrustAsia SMIME ECC CA 2024 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	E1B057357F7 E7E7FC8B108 D39AA6D1F95 1EB9AA3	E21C0762F0B 1777AB2B06E 9F9273BE251 AB9FBB3D5DD 901F60750EF 9B53B8488	TrustAsia SMIME ECC Root CA
CN = TrustAsia TSA RSA Root CA O = TrustAsia Technologies, Inc. C = CN	Root Key	sha384RSA	4096 bits	38DC7012944 4CD6C205E3F D26AE5A4B3F 9EFAFA0	1498BFED947 C795235D348 2FBE493CD89 BE5DC074729 1C716360356 E89D4595E	TrustAsia TSA RSA Root CA
CN = TrustAsia TSA RSA CA 2024 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	81F63777034 F1EB469416D FFA4BB363AE E24E131	6AC8AF44575 A99945D01DD 0BD67527724 2D7DD1A515A 84D68E530EC 5000363C6	TrustAsia TSA RSA Root CA
CN = TrustAsia TSA ECC Root CA O = TrustAsia Technologies, Inc. C = CN	Root Key	sha384ECDSA	384 bits	25A66C22F38 0042663336C FD25A41E473 4FDFB6E	2E04BF6C4C9 1864389F7CB 30AFF4B5434 6794EF897B0 D6557F10B7A 8BA6D932C	TrustAsia TSA ECC Root CA
CN = TrustAsia TSA ECC CA 2024 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	D080C71A271 6F07AFC00D4 50A1AAC5F22 FB3179D	03053C0713B 9543C40B233 1FF5B571270 DF729B41087 DF450BCE44F 455AB8158	TrustAsia TSA ECC Root CA

Appendix B

Applicable versions of Certification Practice Statement (CPS) and Certificate Policy (CP) in-scope:

Name	Version	Date
TrustAsia Certificate Policy and Certification Practice Statement for Global Trusted Service	2.0	23 July 2024
TrustAsia Certificate Policy and Certification Practice Statement for Global Trusted Service	1.7.2	25 April 2024
TrustAsia Certificate Policy and Certification Practice Statement for Global Trusted Service	1.7.1	21 December 2023
TrustAsia Certificate Policy and Certification Practice Statement for Global Trusted Service	1.7.0	30 August 2023
TrustAsia Certificate Policy and Certification Practice Statement for Global Trusted Service	1.6.1	10 February 2023

Appendix C

Locations in-scope:

Location	Function
Shanghai (Central), China	Administration and Support
Shanghai (West), China	Datacenter Facility
Shanghai (East), China	Datacenter Facility

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：亚数信息科技（上海）有限公司管理阶层

我们接受委托，对附件表 A 的所列的亚数信息科技（上海）有限公司（TrustAsia Technologies, Inc.，简称“TrustAsia”）于 2023 年 8 月 1 日至 2024 年 7 月 31 日就 TrustAsia 在附件表 C 所列地点运营的电子认证服务其管理阶层认定执行了合理保证的鉴证业务。根据管理阶层认定，TrustAsia 已：

- 在 CP/CPS 中披露了电子认证业务、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
- 通过有效控制机制，以提供以下合理保证：
 - TrustAsia 的 CPS 与 CP 相符；
 - TrustAsia 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；以及
 - 于 TrustAsia 所执行的注册操作恰当地鉴定 SSL 证书申请者的信息
- 通过有效控制机制，以提供以下合理保证：
 - 对 CA 系统和数据的逻辑和物理访问仅限于授权的个人；
 - 保持密钥和证书管理操作的连续性；以及
 - CA 系统的开发，维护和操作得到适当的授权和执行，以维持 CA 系统的完整

以符合 [WebTrust Principles and Criteria for Certification Authorities, v2.2.2](#)。

TrustAsia 未托管其私钥，亦未提供证书挂起服务。据此，我们的程序未延伸至相关标准的有关控制。

于本审计週期，在与主数据中心位于同一城市的新数据中心投入运营后，TrustAsia 已将生产运营的系统资源从原上海（东）数据中心迁移至此上海（西）新数据中心，并将所有密钥材料从原主数据中心运送至新数据中心，以作为审计范围内密钥材料的新安全位置。新数据中心投入运营并进行了迁移前，相应控制措施的存在和有效性已进行了现场检查，以确保准备就绪与合规性。

TrustAsia 的责任

TrustAsia 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 TrustAsia 所提供的服务能够符合 [WebTrust Principles and Criteria for Certification Authorities, v2.2.2](#) 的规定。

审计师的独立性和质量控制

我们保持独立性并遵守国际道德委员会针对会计人员发布的职业会计师道德准则（*Code of Ethics for Professional Accountants*）规定的道德要求，该准则是建立在正直、客观、专业能力和谨慎、保密和职业行为的基本原则之上。

我们公司遵循国际标准要求的品质管理标准（ISQM）1，并据此维护全面的质量控制体系，包括符合道德要求、专业标准和适用法律法规要求的文件化的政策和程序。

审计师的责任

我们的职责是在执行鉴证工作的基础上对 TrustAsia 的管理层认定发表结论。我们根据国际审计与鉴证准则理事会发布的国际鉴证业务准则第 3000 号“*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。此准则要求我们计划并执行相应的审计程序以获取所有重大方面和对管理层认定的合理保证，包括：

- (1) 了解 TrustAsia 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) 选择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。

我们相信，我们获取的证据是充分、适当的，为发表鉴证结论提供了基础。

控制的有效性

TrustAsia 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。

固有限制

由于内部控制体系本身的限制，TrustAsia 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。

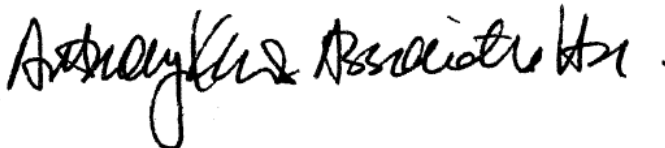
结论

我们认为，TrustAsia 于 2023 年 8 月 1 日至 2024 年 7 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 Principles and Criteria for Certification Authorities, v2.2.2](#)。

本报告并不包括任何在 [WebTrust Principles and Criteria for Certification Authorities, v2.2.2](#) 以外的质量标准声明，或对任何客户对 TrustAsia 服务的合适性声明。

对 Webtrust 标识的使用

在 TrustAsia 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。



Anthony Kam & Associates Ltd.

Certified Public Accountants

2105 Wing On Ctr, 111 Connaught Road, HK SAR, China

14 Oct 2024

KAM Hau Choi Anthony

Practising Certificate Number P02558

附件表 A

本鉴证报告内包括的密钥与证书列举如下:

Subject DN	Key Type	Signature Algorithm	Key Size	Subject Key Identifier	SHA256 Certificate Thumbprints	Certificate Signed by
CN = TrustAsia Global Root CA G1 O = TrustAsia Technologies, Inc. C = CN	Root Key	Sha256RSA	4096 bits	24C20F2CCDC0B5154F6B6D D4F2F058FE1443DFF4	05F82DE4B4A9ED4B7CD1 F3ACE9B73B D6DB69D878 16DD384719 5CF737ED29 51E7	TrustAsia Global Root CA G1
CN = TrustAsia DV TLS RSA CA O = TrustAsia Technologies, Inc. C = CN	Signing Key	Sha256RSA	4096 bits	BF3FDED0466D4A50CFE2FB E20B854834C1AFB825	322C1AFDCC9827AC4D23 4780082A98 6203494199 8AFF67E6D7 7BC4C560DB 25B4	TrustAsia Global Root CA G1
CN = TrustAsia OV TLS RSA CA O = TrustAsia Technologies, Inc. C = CN	Signing Key	Sha256RSA	4096 bits	EFD7A5E0375A8E6A5D60CF BBDDFE80F2383985EA	624FD02328D23289573E BA7D184525 8D70E15BC2 81E7DA38DC E06A5712B2 54A1	TrustAsia Global Root CA G1
CN = TrustAsia EV TLS RSA CA O = TrustAsia Technologies, Inc. C = CN	Signing Key	Sha256RSA	4096 bits	9C95683DD43AC03DD2BA2B AC315C4CAD53BC90CD	853B06C42E26160305CC 3DD5B1F7F7 DC6BAC5602 C0F444F08D 45A7DEE1F4 7CF8	TrustAsia Global Root CA G1
CN = TrustAsia Code Signing RSA CA O = TrustAsia Technologies, Inc. C = CN	Signing Key	Sha256RSA	4096 bits	F1ECAF24AAAE1F2958F17 2AB838B9F86FC394B9	4A14A381B9F2E7A7A49E FA3A87360D B433C6DAF7 B80E06F675 72EA892437 5B60	TrustAsia Global Root CA G1
CN = TrustAsia EV Code Signing RSA CA O = TrustAsia Technologies, Inc. C = CN	Signing Key	Sha256RSA	4096 bits	4B2572DF664CBD56C3F9FB ED36BC287E29AE0326	982222E6B2485A0A80C1 7209630EA9 749B8785E6 C75D6475B3 E4AA578D90 1DF5	TrustAsia Global Root CA G1
CN = TrustAsia Document Signing RSA CA O = TrustAsia Technologies, Inc. C = CN	Signing Key	Sha256RSA	4096 bits	68752DEB635AC881EFC268 430CF215C5564D63E5	033C44B6C711CA26E7B5 ABFD36B721 10F5944146 D99E92C020 266B90FDD7 66A6	TrustAsia Global Root CA G1

CN = TrustAsia Secure Email RSA CA O = TrustAsia Technologies, Inc. C = CN	Signing Key	Sha256RSA	4096 bits	FCB3E33D448 455D2FF172D 1C4DF961090 3C6D94A	E67767E9C72 E0691497F66 616590D99AF DC60974FE6F 1F4F1BFD71B 2A13E2C03	TrustAsia Global Root CA G1
CN = TrustAsia TimeStamping RSA CA O = TrustAsia Technologies, Inc. C = CN	Signing Key	Sha256RSA	4096 bits	7F0BBE8BB42 329F2811B0A 538415ABCE6 27E5BD8	748F6BD8667 C2158C3E384 27D9039BE0B C4C016EF0BE EB73B8BDF0 42B343974	TrustAsia Global Root CA G1
CN = TrustAsia Global Root CA G2 O = TrustAsia Technologies, Inc. C = CN	Root Key	sha384ECDSA	384 bits	4FEB2996F4F 142DE5AA207 56B2FF59C28 53EC398	1DF7E8B185C A46578D458D 05129854FDE 32EF1E9B36F 0B96963CE38 CAEABE4BC	TrustAsia Global Root CA G2
CN = TrustAsia DV TLS ECC CA O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	C12D72D0E89 25B196052C0 DCEE6A734D2 1191706	C3D06E52712 33ED46A538C 150FDCDCD73 F88AECF624 B8D16F981C1 3742E924D	TrustAsia Global Root CA G2
CN = TrustAsia OV TLS ECC CA O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	F3118C08803 CE2E7D69301 9F7D422BAC7 B4DE39F	5655EAAF713 3936558CADD E8F3447615F 759C9C63BEE 949D4DC3CD7 FB71FCBED	TrustAsia Global Root CA G2
CN = TrustAsia EV TLS ECC CA O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	1C72953489D 756FE3D84BD AD33B51C1DD 9472536	2126C130F1D 576FB70CF3B 8E8C0EA2FEE 8CFE98D7213 04EAAA6D898 E721029CE	TrustAsia Global Root CA G2
CN = TrustAsia Global Root CA G3 O = TrustAsia Technologies, Inc. C = CN	Root Key	sha384RSA	4096 bits	40E4E4F223E F38CAB0AE57 7FF22130163 4DBBC92	E0D3226AEB 1163C2E48F F9BE3B50B4 C6431BE7BB 1EACC5C36B 5D5EC50903 9A08	TrustAsia Global Root CA G3
CN = TrustAsia DV TLS RSA CA G3 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	FFD38BE629C 8A6994DE519 6BF8FFAF394 19D7ED6	E0DD6743D6 D08E2AB188 84ED1E7E46 B3D9726FFF A9B1866642 AEBF266FDA 2654	TrustAsia Global Root CA G3

CN = TrustAsia OV TLS RSA CA G3 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	22AADBB42F7 F3C183F717E CD61FD4ECE4 656EF54	573F5F7974 82F567EDC7 901879457B C46C9DF0AC FD8CE7B1A8 FB7E2218FA 477B	TrustAsia Global Root CA G3
CN = TrustAsia EV TLS RSA CA G3 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	22C292A6316 3AC13C7176A 4F313B25727 37CD26A	15DDF98C57 E0F46E5C5E E00283BC4A F8FE0E8D2C 42151630DE FFFA285EA6 2D09	TrustAsia Global Root CA G3
CN = TrustAsia Code Signing RSA CA G3 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	A3ED9A5FE3D FE8CE6AB41E C63C625FDCA C9A0682	FA012B12A4 53DAF7C02B D7F8FF617A 4C91EB2953 D3E42F6FDB 000EAE4FB6 FAAE	TrustAsia Global Root CA G3
CN = TrustAsia EV Code Signing RSA CA G3 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	217C9E5F581 AC037C9EEAC CADA99DB861 393B1C3	DD169948C5 6F90D640E3 92F7A69452 EC4B394E6A D179FF54F7 E7DBB6AACF BDBA	TrustAsia Global Root CA G3
CN = TrustAsia Document Signing RSA CA G3 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	0521A508833 75645B4055F 1B6D206127D 85E8143	B7DE90291B 7905CBDB8C 744E98F1E6 FC97C2288B 2177F79D91 6D18D31AE8 B2A7	TrustAsia Global Root CA G3
CN = TrustAsia Secure Email RSA CA G3 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	EB164C7D748 A091C5787C3 5B9B98FF213 6C3B20A	C84E9EE5225 DF7B674A573 43C6D489219 07E97640100 42E40B2C00F 944639CA4	TrustAsia Global Root CA G3
CN = TrustAsia TimeStamping RSA CA G3 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	8BEE09E649C 638F4A45176 DBAE1B1013A F231775	904A794C751 20499475947 46743265348 A339A7573E2 323B9D4BE89 BBFAFA5D52	TrustAsia Global Root CA G3
CN = TrustAsia Global Root CA G4 O = TrustAsia Technologies, Inc. C = CN	Root Key	sha384ECDSA	384 bits	A5BB4A97CEB 32B7FA431DE 97835983A66 F71CBDE	BE4B56CB505 6C0136A526D F444508DAA3 6A0B54F42E4 AC38F72AF47 0E479654C	TrustAsia Global Root CA G4

CN = TrustAsia DV TLS ECC CA G4 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	0C09D741BDF 04CB767E4B0 56BF7E8DB91 433322F	C28348740DA 36CF14DDC49 280CF030AB9 CE3B0ACE093 B0E1BA18945 6F4918B9C	TrustAsia Global Root CA G4
CN = TrustAsia OV TLS ECC CA G4 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	76533221F36 F769D585329 33BEF548B9E 2284FEF	EEE6BAF50B1 4BCA04202B4 96737E676F7 13E7431FFD4 FCA1309F661 481EC520F	TrustAsia Global Root CA G4
CN = TrustAsia EV TLS ECC CA G4 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	EF46439CE9F 4121DF11A18 1968571D84B AAF7D19	C261EE3D4BB DC456FFB678 68363FED80C B5C9AD7AF3F 5A5DACBE32B ECDD88A7	TrustAsia Global Root CA G4
CN = TrustAsia Code Signing ECC CA G4 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	FB7514C9DD3 5A7003A3C13 54259BFDDE3 F02DCF6	933ECE2B4EB B0557072C7B 408F6D36A54 0524C3D1A60 F260C97D962 9D060BA7B	TrustAsia Global Root CA G4
CN = TrustAsia EV Code Signing ECC CA G4 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	C722B5F7C34 ADC9B2C1958 5BC16672266 36CF4E3	6A423235B3B 26C7DED5359 BF0BAD4EE30 1729DAF8287 244FC9995B0 605268EDB	TrustAsia Global Root CA G4
CN = TrustAsia Document Signing ECC CA G4 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	DEA970A22DB 35572EB5849 77653F23479 C4F74A1	84598841793 B351DD3AD8C 11A521CAD00 270CF64663C 80002A02557 2F8020792	TrustAsia Global Root CA G4
CN = TrustAsia Secure Email ECC CA G4 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	613250574BF 3266AE9C8D7 C61337F17E1 553B3AC	70342F6C5E0 FD9F9ABE3C1 448D033E1A0 CAB4CC56040 9E1C03B626E 48B8B16DD	TrustAsia Global Root CA G4
CN = TrustAsia TimeStamping ECC CA G4 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	6CDF8F267CE 820FE629B3F A81F15EEEA7 CF54C46	B917AB79332 B73B9386552 89C287F183E 55B1BC60873 845ABA119DB 93D2E3C08	TrustAsia Global Root CA G4

CN = TrustAsia TLS RSA Root CA O = TrustAsia Technologies, Inc. C = CN	Root Key	sha384RSA	4096 bits	B80791795C0 6F446FD7B59 CA5A2691A74 52BF853	06C08D7DAFD 876971EB112 4FE67F847EC 0C7A158D3EA 53CBE940E2E A9791F4C3	TrustAsia TLS RSA Root CA
CN = TrustAsia DV TLS RSA CA 2024 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	6175054E1AF 50FC1602020 C228D98BB3E 2C17DB4	5EB0217B928 C2DE1170FCE 110CACC3C89 A42492E4F97 F5AE1EB8CD5 4F8A68EEB	TrustAsia TLS RSA Root CA
CN = TrustAsia OV TLS RSA CA 2024 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	967C134272A B3A936C501A EDEE18113A9 F9C250D	D0B626C8AD9 3962296B392 0106ED7FB38 18FCB98E0B7 3E799141B42 521335B0F	TrustAsia TLS RSA Root CA
CN = TrustAsia EV TLS RSA CA 2024 V2 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	5B1A314630D C3325DD9825 8EEF84D189C A4BB826	D886C235FAF ADD2E473492 4CF58B4D8F0 CB7065F0F54 51B3E1C308F 92EF7B2EB	TrustAsia TLS RSA Root CA
CN = TrustAsia TLS ECC Root CA O = TrustAsia Technologies, Inc. C = CN	Root Key	sha384ECDSA	384 bits	2C8553BBB14 3CD32EA9EA3 87FEA298A8A 693E910	C0076B9EF05 31FB1A656D6 7C4EBE97CD5 DBAA41EF445 98ACC248987 8C92D8711	TrustAsia TLS ECC Root CA
CN = TrustAsia DV TLS ECC CA 2024 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	D0B70CEDFC5 402C2C05D7E 3B17EBBF105 0B19665	73E9BE7D57B D5C72A06304 463D32F8F85 ECA12E2F2D2 84E48AE83F6 53FDB4EB6	TrustAsia TLS ECC Root CA
CN = TrustAsia OV TLS ECC CA 2024 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	A4534BA525B AAA848E0B87 9DC94EAA3AD D0EBAC6	0E975E62A83 030EAE3F441 BAFFBFD7574 FB7235EECB5 0F1F747DF8F 0506D245E	TrustAsia TLS ECC Root CA
CN = TrustAsia EV TLS ECC CA 2024 V2 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	8E8ECB35F18 158AA202DCE C336168A101 13859C7	D19E1FCD8E1 2747D75B74A 28318EEFDD7 00F616E2B21 5701BBE804C 3CDDA027B	TrustAsia TLS ECC Root CA

CN = TrustAsia CS RSA Root CA O = TrustAsia Technologies, Inc. C = CN	Root Key	sha384RSA	4096 bits	B12E11466A8 2339CD3F2F0 018529A607B 792A79E	F38AB64B30C 0D900B7212A 793651B87F2 87C57522400 7F3B8851618 FD5B48DEB	TrustAsia CS RSA Root CA
CN = TrustAsia CS RSA CA 2024 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	7EB2529B31F 4F4B4F7D5BE 0F831028CD6 8C08AAE	0C67D64F643 0F927EB3772 677ADFC5C23 6A14E3DF7A7 66BFF299FB7 EAB1EF315	TrustAsia CS RSA Root CA
CN = TrustAsia CS ECC Root CA O = TrustAsia Technologies, Inc. C = CN	Root Key	sha384ECDSA	384 bits	5D875EB48E9 6795EB534A5 42B1C3798F7 35DEF4B	6B9C91E5A64 53375EF905D 8F2A5369953 065F471664F 2E676E2013D F388C9B56	TrustAsia CS ECC Root CA
CN = TrustAsia CS ECC CA 2024 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	708C1FD8C6B 1AA07387BA7 8F3BAA23039 9AE53C1	5CF4B9BC8D9 BA4A96DE8BC 3B5C38D0372 B0A0187DD1A 9AE985647A8 1F077610B	TrustAsia CS ECC Root CA
CN = TrustAsia SMIME RSA Root CA O = TrustAsia Technologies, Inc. C = CN	Root Key	sha384RSA	4096 bits	801AAA43C1C 97F8B1A9645 BC3DBB6B485 26C5BAB	C7796BEB62C 101BB143D26 2A7C96A0C61 68183223EF5 0D699632D86 E03B8CC9B	TrustAsia SMIME RSA Root CA
CN = TrustAsia SMIME RSA CA 2024 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	20741B3D532 5D2968E2846 8167E43DB50 550784B	BC2197C0C1F F17C553370B F9955B9B50C 8C9D27A0C28 F78704E00C8 81F1458AA	TrustAsia SMIME RSA Root CA
CN = TrustAsia SMIME ECC Root CA O = TrustAsia Technologies, Inc. C = CN	Root Key	sha384ECDSA	384 bits	3167E672B20 DE622A0ACCF 7E22A75932E 36623A5	436472C1009 A325C54F1A5 BBB5468A7BA EECCBE05DE5 F099CB70D3F E41E13C16	TrustAsia SMIME ECC Root CA
CN = TrustAsia SMIME ECC CA 2024 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	E1B057357F7 E7E7FC8B108 D39AA6D1F95 1EB9AA3	E21C0762F0B 1777AB2B06E 9F9273BE251 AB9FBB3D5DD 901F60750EF 9B53B8488	TrustAsia SMIME ECC Root CA

CN = TrustAsia TSA RSA Root CA O = TrustAsia Technologies, Inc. C = CN	Root Key	sha384RSA	4096 bits	38DC7012944 4CD6C205E3F D26AE5A4B3F 9EFAFA0	1498BFED947 C795235D348 2FBE493CD89 BE5DC074729 1C716360356 E89D4595E	TrustAsia TSA RSA Root CA
CN = TrustAsia TSA RSA CA 2024 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	81F63777034 F1EB469416D FFA4BB363AE E24E131	6AC8AF44575 A99945D01DD 0BD67527724 2D7DD1A515A 84D68E530EC 5000363C6	TrustAsia TSA RSA Root CA
CN = TrustAsia TSA ECC Root CA O = TrustAsia Technologies, Inc. C = CN	Root Key	sha384ECDSA	384 bits	25A66C22F38 0042663336C FD25A41E473 4FD6B6E	2E04BF6C4C9 1864389F7CB 30AFF4B5434 6794EF897B0 D6557F10B7A 8BA6D932C	TrustAsia TSA ECC Root CA
CN = TrustAsia TSA ECC CA 2024 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	D080C71A271 6F07AFC00D4 50A1AAC5F22 FB3179D	03053C0713B 9543C40B233 1FF5B571270 DF729B41087 DF450BCE44F 455AB8158	TrustAsia TSA ECC Root CA

附件表 B

范围内适用之 CP/CPS 版本:

Name	Version	Date
TrustAsia Certificate Policy and Certification Practice Statement for Global Trusted Service	2.0	23 July 2024
TrustAsia Certificate Policy and Certification Practice Statement for Global Trusted Service	1.7.2	25 April 2024
TrustAsia Certificate Policy and Certification Practice Statement for Global Trusted Service	1.7.1	21 December 2023
TrustAsia Certificate Policy and Certification Practice Statement for Global Trusted Service	1.7.0	30 August 2023
TrustAsia Certificate Policy and Certification Practice Statement for Global Trusted Service	1.6.1	10 February 2023

附件表 C

范围内地点:

地点	功能
中国上海(中)	管理与支持
中国上海(西)	数据中心
中国上海(东)	数据中心

管理阶层认定报告

(本中文报告只作参考，正文请参阅英文报告)

亚数信息科技 (上海) 有限公司 (以下简称 “ TrustAsia ”) 运营电子认证服务机构 (以下简称 “ CA ” ，附件表 A 列举了服务所包括的根证书和中级证书) ，并提供以下电子认证服务：

- 订户注册
- 证书更新
- 证书密钥更新
- 证书发布
- 证书分发
- 证书吊销
- 证书验证

TrustAsia 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、以及证书生命周期管理。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 TrustAsia 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。

TrustAsia 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，TrustAsia 管理层认为，在 2023 年 8 月 1 日至 2024 年 7 月 31 日就 TrustAsia 在附件表 C 所列地点提供电子认证服务期间，TrustAsia 已：

- 在附件表 B 之 CP/CPS 中披露了电子认证业务、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
- 通过有效控制机制，以提供以下合理保证：
 - TrustAsia 的 CPS 与 CP 相符；以及
 - TrustAsia 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；以及
 - 于 TrustAsia 所执行的注册操作恰当地鉴定证书申请者的信息；
- 通过有效控制机制，以提供以下合理保证：

- 对 CA 系统和数据的逻辑和物理访问仅限于授权的个人；
- 保持密钥和证书管理操作的连续性；以及
- CA 系统的开发、维护和操作得到适当的授权和执行，以维持 CA 系统的完整；

以符合 [WebTrust Principles and Criteria for Certification Authorities 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
 - 系统开发与维护管理
 - 业务持续性管理
 - 监控与合规管理
 - 审计日志管理
- **CA 密钥生命周期管理**
 - CA 密钥生成
 - CA 密钥存储、备份和恢复
 - CA 公钥分发
 - CA 密钥使用
 - CA 密钥归档和销毁
 - CA 密钥泄露
 - CA 密码设备生命周期管理
- **证书生命周期管理**
 - 订户注册
 - 证书更新
 - 证书密钥更新

- 证书发布
- 证书分发
- 证书吊销
- 证书验证

TrustAsia 未托管其私钥，亦未提供证书挂起服务。因此，我们的认定报告未延伸至相关标准的有关控制。

于本审计週期，在与主数据中心位于同一城市的新数据中心投入运营后，TrustAsia 已将生产运营的系统资源从原上海（东）数据中心迁移至此上海（西）新数据中心，并将所有密钥材料从原主数据中心运送至新数据中心，以作为审计范围内密钥材料的新安全位置。新数据中心投入运营并进行了迁移前，相应控制措施的存在和有效性已进行了现场检查，以确保准备就绪与合规性。

总经理 翟新元

亚数信息科技（上海）有限公司
上海市徐汇区桂平路 391 号 B 座 32 层

2024 年 10 月 14 日



附件表 A

本认定报告内包括的密钥与证书列举如下:

Subject DN	Key Type	Signature Algorithm	Key Size	Subject Key Identifier	SHA256 Certificate Thumbprints	Certificate Signed by
CN = TrustAsia Global Root CA G1 O = TrustAsia Technologies, Inc. C = CN	Root Key	Sha256RSA	4096 bits	24C20F2CCDC 0B5154F6B6D D4F2F058FE1 443DFF4	05F82DE4B4 A9ED4B7CD1 F3ACE9B73B D6DB69D878 16DD384719 5CF737ED29 51E7	TrustAsia Global Root CA G1
CN = TrustAsia DV TLS RSA CA O = TrustAsia Technologies, Inc. C = CN	Signing Key	Sha256RSA	4096 bits	BF3FDED0466 D4A50CFE2FB E20B854834C 1AFB825	322C1AFDCC 9827AC4D23 4780082A98 6203494199 8AFF67E6D7 7BC4C560DB 25B4	TrustAsia Global Root CA G1
CN = TrustAsia OV TLS RSA CA O = TrustAsia Technologies, Inc. C = CN	Signing Key	Sha256RSA	4096 bits	EFD7A5E0375 A8E6A5D60CF BBDDFE80F23 83985EA	624FD02328 D23289573E BA7D184525 8D70E15BC2 81E7DA38DC E06A5712B2 54A1	TrustAsia Global Root CA G1
CN = TrustAsia EV TLS RSA CA O = TrustAsia Technologies, Inc. C = CN	Signing Key	Sha256RSA	4096 bits	9C95683DD43 AC03DD2BA2B AC315C4CAD5 3BC90CD	853B06C42E 26160305CC 3DD5B1F7F7 DC6BAC5602 C0F444F08D 45A7DEE1F4 7CF8	TrustAsia Global Root CA G1
CN = TrustAsia Code Signing RSA CA O = TrustAsia Technologies, Inc. C = CN	Signing Key	Sha256RSA	4096 bits	F1ECAAF24AAA EE1F2958F17 2AB838B9F86 FC394B9	4A14A381B9 F2E7A7A49E FA3A87360D B433C6DAF7 B80E06F675 72EA892437 5B60	TrustAsia Global Root CA G1
CN = TrustAsia EV Code Signing RSA CA O = TrustAsia Technologies, Inc. C = CN	Signing Key	Sha256RSA	4096 bits	4B2572DF664 CBD56C3F9FB ED36BC287E2 9AE0326	982222E6B2 485A0A80C1 7209630EA9 749B8785E6 C75D6475B3 E4AA578D90 1DF5	TrustAsia Global Root CA G1
CN = TrustAsia Document Signing RSA CA O = TrustAsia Technologies, Inc. C = CN	Signing Key	Sha256RSA	4096 bits	68752DEB635 AC881EFC268 430CF215C55 64D63E5	033C44B6C7 11CA26E7B5 ABFD36B721 10F5944146 D99E92C020 266B90FDD7 66A6	TrustAsia Global Root CA G1
CN = TrustAsia Secure Email RSA CA O = TrustAsia Technologies, Inc. C = CN	Signing Key	Sha256RSA	4096 bits	FCB3E33D448 455D2FF172D 1C4DF961090 3C6D94A	E67767E9C72 E0691497F66 616590D99AF DC60974FE6F 1F4F1BFD71B 2A13E2C03	TrustAsia Global Root CA G1

CN = TrustAsia TimeStamping RSA CA O = TrustAsia Technologies, Inc. C = CN	Signing Key	Sha256RSA	4096 bits	7F0BBE8BB42 329F2811B0A 538415ABCE6 27E5BD8	748F6BD8667 C2158C3E384 27D9039BE0B C4C016EF0BE EB73B8BDDFF0 42B343974	TrustAsia Global Root CA G1
CN = TrustAsia Global Root CA G2 O = TrustAsia Technologies, Inc. C = CN	Root Key	sha384ECDSA	384 bits	4FEB2996F4F 142DE5AA207 56B2FF59C28 53EC398	1DF7E8B185C A46578D458D 05129854FDE 32EF1E9B36F 0B96963CE38 CAEABE4BC	TrustAsia Global Root CA G2
CN = TrustAsia DV TLS ECC CA O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	C12D72D0E89 25B196052C0 DCEE6A734D2 1191706	C3D06E52712 33ED46A538C 150FDCDCD73 F88AECE624 B8D16F981C1 3742E924D	TrustAsia Global Root CA G2
CN = TrustAsia OV TLS ECC CA O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	F3118C08803 CE2E7D69301 9F7D422BAC7 B4DE39F	5655EAAF713 3936558CADD E8F3447615F 759C9C63BEE 949D4DC3CD7 FB71FCBED	TrustAsia Global Root CA G2
CN = TrustAsia EV TLS ECC CA O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	1C72953489D 756FE3D84BD AD33B51C1DD 9472536	2126C130F1D 576FB70CF3B 8E8C0EA2FEE 8CFE98D7213 04EAAA6D898 E721029CE	TrustAsia Global Root CA G2
CN = TrustAsia Global Root CA G3 O = TrustAsia Technologies, Inc. C = CN	Root Key	sha384RSA	4096 bits	40E4E4F223E F38CAB0AE57 7FF22130163 4DBBC92	E0D3226AEB 1163C2E48F F9BE3B50B4 C6431BE7BB 1EACC5C36B 5D5EC50903 9A08	TrustAsia Global Root CA G3
CN = TrustAsia DV TLS RSA CA G3 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	FFD38BE629C 8A6994DE519 6BF8FFAF394 19D7ED6	E0DD6743D6 D08E2AB188 84ED1E7E46 B3D9726FFF A9B1866642 AEBF266FDA 2654	TrustAsia Global Root CA G3
CN = TrustAsia OV TLS RSA CA G3 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	22AADBB42F7 F3C183F717E CD61FD4ECE4 656EF54	573F5F7974 82F567EDC7 901879457B C46C9DF0AC FD8CE7B1A8 FB7E2218FA 477B	TrustAsia Global Root CA G3
CN = TrustAsia EV TLS RSA CA G3 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	22C292A6316 3AC13C7176A 4F313B25727 37CD26A	15DDF98C57 E0F46E5C5E E00283BC4A F8FE0E8D2C 42151630DE FFFA285EA6 2D09	TrustAsia Global Root CA G3

CN = TrustAsia Code Signing RSA CA G3 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	A3ED9A5FE3D FE8CE6AB41E C63C625FDCA C9A0682	FA012B12A4 53DAF7C02B D7F8FF617A 4C91EB2953 D3E42F6FDB 000EAE4FB6 FAAE	TrustAsia Global Root CA G3
CN = TrustAsia EV Code Signing RSA CA G3 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	217C9E5F581 AC037C9EEAC CADA99DB861 393B1C3	DD169948C5 6F90D640E3 92F7A69452 EC4B394E6A D179FF54F7 E7DBB6AACF BDBA	TrustAsia Global Root CA G3
CN = TrustAsia Document Signing RSA CA G3 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	0521A508833 75645B4055F 1B6D206127D 85E8143	B7DE90291B 7905CBDB8C 744E98F1E6 FC97C2288B 2177F79D91 6D18D31AE8 B2A7	TrustAsia Global Root CA G3
CN = TrustAsia Secure Email RSA CA G3 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	EB164C7D748 A091C5787C3 5B9B98FF213 6C3B20A	C84E9EE5225 DF7B674A573 43C6D489219 07E97640100 42E40B2C00F 944639CA4	TrustAsia Global Root CA G3
CN = TrustAsia TimeStamping RSA CA G3 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	8BEE09E649C 638F4A45176 DBAE1B1013A F231775	904A794C751 20499475947 46743265348 A339A7573E2 323B9D4BE89 BBAFA5D52	TrustAsia Global Root CA G3
CN = TrustAsia Global Root CA G4 O = TrustAsia Technologies, Inc. C = CN	Root Key	sha384ECDSA	384 bits	A5BB4A97CEB 32B7FA431DE 97835983A66 F71CBDE	BE4B56CB505 6C0136A526D F444508DAA3 6A0B54F42E4 AC38F72AF47 0E479654C	TrustAsia Global Root CA G4
CN = TrustAsia DV TLS ECC CA G4 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	0C09D741BDF 04CB767E4B0 56BF7E8DB91 433322F	C28348740DA 36CF14DDC49 280CF030AB9 CE3B0ACE093 B0E1BA18945 6F4918B9C	TrustAsia Global Root CA G4
CN = TrustAsia OV TLS ECC CA G4 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	76533221F36 F769D585329 33BEF548B9E 2284FEF	EEE6BAF50B1 4BCA04202B4 96737E676F7 13E7431FFD4 FCA1309F661 481EC520F	TrustAsia Global Root CA G4
CN = TrustAsia EV TLS ECC CA G4 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	EF46439CE9F 4121DF11A18 1968571D84B AAF7D19	C261EE3D4BB DC456FFB678 68363FED80C B5C9AD7AF3F 5A5DACBE32B ECDDD88A7	TrustAsia Global Root CA G4

CN = TrustAsia Code Signing ECC CA G4 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	FB7514C9DD3 5A7003A3C13 54259BFDDE3 F02DCF6	933ECE2B4EB B0557072C7B 408F6D36A54 0524C3D1A60 F260C97D962 9D060BA7B	TrustAsia Global Root CA G4
CN = TrustAsia EV Code Signing ECC CA G4 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	C722B5F7C34 ADC9B2C1958 5BC16672266 36CF4E3	6A423235B3B 26C7DED5359 BF0BAD4EE30 1729DAF8287 244FC9995B0 605268EDB	TrustAsia Global Root CA G4
CN = TrustAsia Document Signing ECC CA G4 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	DEA970A22DB 35572EB5849 77653F23479 C4F74A1	84598841793 B351DD3AD8C 11A521CAD00 270CF64663C 80002A02557 2F8020792	TrustAsia Global Root CA G4
CN = TrustAsia Secure Email ECC CA G4 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	613250574BF 3266AE9C8D7 C61337F17E1 553B3AC	70342F6C5E0 FD9F9ABE3C1 448D033E1A0 CAB4CC56040 9E1C03B626E 48B8B16DD	TrustAsia Global Root CA G4
CN = TrustAsia TimeStamping ECC CA G4 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	6CDF8F267CE 820FE629B3F A81F15EEEA7 CF54C46	B917AB79332 B73B9386552 89C287F183E 55B1BC60873 845ABA119DB 93D2E3C08	TrustAsia Global Root CA G4
CN = TrustAsia TLS RSA Root CA O = TrustAsia Technologies, Inc. C = CN	Root Key	sha384RSA	4096 bits	B80791795C0 6F446FD7B59 CA5A2691A74 52BF853	06C08D7DAFD 876971EB112 4FE67F847EC 0C7A158D3EA 53CBE940E2E A9791F4C3	TrustAsia TLS RSA Root CA
CN = TrustAsia DV TLS RSA CA 2024 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	6175054E1AF 50FC1602020 C228D98BB3E 2C17DB4	5EB0217B928 C2DE1170FCE 110CACC3C89 A42492E4F97 F5AE1EB8CD5 4F8A68EEB	TrustAsia TLS RSA Root CA
CN = TrustAsia OV TLS RSA CA 2024 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	967C1342724 B3A936C501A EDEE18113A9 F9C250D	D0B626C8AD9 3962296B392 0106ED7FB38 18FCB98E0B7 3E799141B42 521335B0F	TrustAsia TLS RSA Root CA
CN = TrustAsia EV TLS RSA CA 2024 V2 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	5B1A314630D C3325DD9825 8EEF84D189C A4BB826	D886C235FAF ADD2E473492 4CF58B4D8F0 CB7065F0F54 51B3E1C308F 92EF7B2EB	TrustAsia TLS RSA Root CA

CN = TrustAsia TLS ECC Root CA O = TrustAsia Technologies, Inc. C = CN	Root Key	sha384ECDSA	384 bits	2C8553BBB14 3CD32EA9EA3 87FEA298A8A 693E910	C0076B9EF05 31FB1A656D6 7C4EBE97CD5 DBAA41EF445 98ACC248987 8C92D8711	TrustAsia TLS ECC Root CA
CN = TrustAsia DV TLS ECC CA 2024 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	D0B70CEDFC5 402C2C05D7E 3B17EBBF105 0B19665	73E9BE7D57B D5C72A06304 463D32F8F85 ECA12E2F2D2 84E48AE83F6 53FDB4EB6	TrustAsia TLS ECC Root CA
CN = TrustAsia OV TLS ECC CA 2024 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	A4534BA525B AAA848E0B87 9DC94EAA3AD D0EBAC6	0E975E62A83 030EAE3F441 BAFFBFD7574 FB7235EECB5 0F1F747DF8F 0506D245E	TrustAsia TLS ECC Root CA
CN = TrustAsia EV TLS ECC CA 2024 V2 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	8E8ECB35F18 158AA202DCE C336168A101 13859C7	D19E1FCD8E1 2747D75B74A 28318EEFDD7 00F616E2B21 5701BBE804C 3CDDA027B	TrustAsia TLS ECC Root CA
CN = TrustAsia CS RSA Root CA O = TrustAsia Technologies, Inc. C = CN	Root Key	sha384RSA	4096 bits	B12E11466A8 2339CD3F2F0 018529A607B 792A79E	F38AB64B30C 0D900B7212A 793651B87F2 87C57522400 7F3B8851618 FD5B48DEB	TrustAsia CS RSA Root CA
CN = TrustAsia CS RSA CA 2024 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	7EB2529B31F 4F4B4F7D5BE 0F831028CD6 8C08AAE	0C67D64F643 0F927EB3772 677ADFC5C23 6A14E3DF7A7 66BFF299FB7 EAB1EF315	TrustAsia CS RSA Root CA
CN = TrustAsia CS ECC Root CA O = TrustAsia Technologies, Inc. C = CN	Root Key	sha384ECDSA	384 bits	5D875EB48E9 6795EB534A5 42B1C3798F7 35DEF4B	6B9C91E5A64 53375EF905D 8F2A5369953 065F471664F 2E676E2013D F388C9B56	TrustAsia CS ECC Root CA
CN = TrustAsia CS ECC CA 2024 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	708C1FD8C6B 1AA07387BA7 8F3BAA23039 9AE53C1	5CF4B9BC8D9 BA4A96DE8BC 3B5C38D0372 B0A0187DD1A 9AE985647A8 1F077610B	TrustAsia CS ECC Root CA
CN = TrustAsia SMIME RSA Root CA O = TrustAsia Technologies, Inc. C = CN	Root Key	sha384RSA	4096 bits	801AAA43C1C 97F8B1A9645 BC3DDB6B485 26C5BAB	C7796BEB62C 101BB143D26 2A7C96A0C61 68183223EF5 0D699632D86 E03B8CC9B	TrustAsia SMIME RSA Root CA

CN = TrustAsia SMIME RSA CA 2024 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	20741B3D532 5D2968E2846 8167E43DB50 550784B	BC2197C0C1F F17C553370B F9955B9B50C 8C9D27A0C28 F78704E00C8 81F1458AA	TrustAsia SMIME RSA Root CA
CN = TrustAsia SMIME ECC Root CA O = TrustAsia Technologies, Inc. C = CN	Root Key	sha384ECDSA	384 bits	3167E672B20 DE622A0ACCF 7E22A75932E 36623A5	436472C1009 A325C54F1A5 BBB5468A7BA EECCBE05DE5 F099CB70D3F E41E13C16	TrustAsia SMIME ECC Root CA
CN = TrustAsia SMIME ECC CA 2024 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	E1B057357F7 E7E7FC8B108 D39AA6D1F95 1EB9AA3	E21C0762F0B 1777AB2B06E 9F9273BE251 AB9FBB3D5DD 901F60750EF 9B53B8488	TrustAsia SMIME ECC Root CA
CN = TrustAsia TSA RSA Root CA O = TrustAsia Technologies, Inc. C = CN	Root Key	sha384RSA	4096 bits	38DC7012944 4CD6C205E3F D26AE5A4B3F 9EFAFA0	1498BFED947 C795235D348 2FBE493CD89 BE5DC074729 1C716360356 E89D4595E	TrustAsia TSA RSA Root CA
CN = TrustAsia TSA RSA CA 2024 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	81F63777034 F1EB469416D FFA4BB363AE E24E131	6AC8AF44575 A99945D01DD 0BD67527724 2D7DD1A515A 84D68E530EC 5000363C6	TrustAsia TSA RSA Root CA
CN = TrustAsia TSA ECC Root CA O = TrustAsia Technologies, Inc. C = CN	Root Key	sha384ECDSA	384 bits	25A66C22F38 0042663336C FD25A41E473 4FDFB6E	2E04BF6C4C9 1864389F7CB 30AFF4B5434 6794EF897B0 D6557F10B7A 8BA6D932C	TrustAsia TSA ECC Root CA
CN = TrustAsia TSA ECC CA 2024 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	D080C71A271 6F07AFC00D4 50A1AAC5F22 FB3179D	03053C0713B 9543C40B233 1FF5B571270 DF729B41087 DF450BCE44F 455AB8158	TrustAsia TSA ECC Root CA

附件表 B

范围内适用之 CP/CPS 版本:

Name	Version	Date
TrustAsia Certificate Policy and Certification Practice Statement for Global Trusted Service	2.0	23 July 2024
TrustAsia Certificate Policy and Certification Practice Statement for Global Trusted Service	1.7.2	25 April 2024
TrustAsia Certificate Policy and Certification Practice Statement for Global Trusted Service	1.7.1	21 December 2023
TrustAsia Certificate Policy and Certification Practice Statement for Global Trusted Service	1.7.0	30 August 2023
TrustAsia Certificate Policy and Certification Practice Statement for Global Trusted Service	1.6.1	10 February 2023

附件表 C

范围内地点:

地点	功能
中国上海(中)	管理与支持
中国上海(西)	数据中心
中国上海(东)	数据中心

INDEPENDENT ASSURANCE REPORT

To the management of TrustAsia Technologies, Inc. ("TrustAsia"):

We have been engaged, in a reasonable assurance engagement, to report on TrustAsia management's assertion that for its Certification Authority (CA) operations at locations as enumerated in Appendix C, throughout the period 1 August 2023 to 31 July 2024 for its CAs as enumerated in Appendix A, TrustAsia has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its Certification Practice Statement (CPS) and Certificate Policy (CP) as enumerated in Appendix B
- maintained effective controls to provide reasonable assurance that:
 - TrustAsia's Certification Practice Statement is consistent with its Certificate Policy
 - TrustAsia provides its services in accordance with its Certificate Policy and Certification Practice Statement
- 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; and
 - subscriber information is properly authenticated
- 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](#).

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

After the planned new site within the same city as the main datacenter went into operations during the audit period, TrustAsia had relocated its system resources for production operations from the original data center at Shanghai (East) to the new site at Shanghai (West) and transported all key materials from the original main site to the new site as the new secure location hosting the key materials within the scope. Corresponding controls had been examined for existence and effectiveness physically on site before the new site went into operations and migration conducted for readiness and compliance.

Certification authority's responsibilities

TrustAsia's management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with the [WebTrust Principles and Criteria for Certification Authorities, v2.2.2](#).

Our independence and quality control

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* 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.

The firm applies International Standard on Quality Management (ISQM) 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements* and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Auditor's responsibilities

Our responsibility is to express an opinion on management's assertion based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's assertion is fairly stated, and, accordingly, included:

- (1) obtaining an understanding of TrustAsia'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.

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

Relative effectiveness of controls

The relative effectiveness and significance of specific controls at TrustAsia 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.

Inherent limitations

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

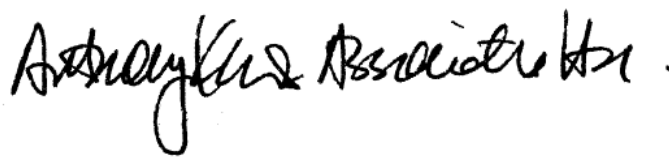
Opinion

In our opinion, throughout the period 1 August 2023 to 31 July 2024, TrustAsia management's assertion, as referred to above, is fairly stated, in all material respects, in accordance with the [WebTrust Principles and Criteria for Certification Authorities, v2.2.2](#).

This report does not include any representation as to the quality of TrustAsia's services beyond those covered by the [WebTrust Principles and Criteria for Certification Authorities, v2.2.2](#), nor the suitability of any of TrustAsia's services for any customer's intended purpose.

Use of the WebTrust seal

TrustAsia'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.



Anthony Kam & Associates Ltd.

Certified Public Accountants

2105 Wing On Ctr, 111 Connaught Road, HK SAR, China

14 Oct 2024

KAM Hau Choi Anthony

Practising Certificate Number P02558

Appendix A

The list of keys and certificates covered in the report is as follow:

Subject DN	Key Type	Signature Algorithm	Key Size	Subject Key Identifier	SHA256 Certificate Thumbprints	Certificate Signed by
CN = TrustAsia Global SM2 Root CA G2 OU = GMCA O = TrustAsia Technologies, Inc. C = CN	Root Key	1.2.156.10197. 1.501	256 bits	58A589F8F9F B2659ABF09A 41D6E6E566D 3A539D6	8C18BBBA69 0D957DE6A5 6AE919335F 443431C1D5 8A8634B336 EE239D381A C933	TrustAsia Global SM2 Root CA G2
CN = TrustAsia TLS SM2 CA G2 OU = GMCA O = TrustAsia Technologies, Inc. C = CN	Signing Key	1.2.156.10197. 1.501	256 bits	9DEDDDD76823 81CA1040138 DC9ABC7993E 2DACB3C	4DD45AEF9D 34D2FBABAC E4D52D33BD 7D1F2143C2 CEFD745FF2 31334FF81C C248	TrustAsia Global SM2 Root CA G2
CN = TrustAsia Device SM2 CA G2 OU = GMCA O = TrustAsia Technologies, Inc. C = CN	Signing Key	1.2.156.10197. 1.501	256 bits	D5794D2BD11 9DEA2E5B47B 5CCB4305F0E 967B7B3	2A02C6A634 801162168D 9C6EC2D79A 9D9EB5C67F E2A417CAE5 C2D8A1B73D B70A	TrustAsia Global SM2 Root CA G2
CN = TrustAsia Identity SM2 CA G2 OU = GMCA O = TrustAsia Technologies, Inc. C = CN	Signing Key	1.2.156.10197. 1.501	256 bits	EA67880B3DB 2B54C78516D 3C858599AD2 7F387D2	9F8E2B6EE1 07A27D7F8F 047ABA0E91 BD29A4D6A5 68E0571B4E 7494345A2E FAB1	TrustAsia Global SM2 Root CA G2
CN = DNSPod TLS SM2 CA G2 O = DNSPod, Inc. C = CN	Signing Key	1.2.156.10197. 1.501	256 bits	C27C7F9AB24 47D17B63819 537951D1168 93B6121	AAE8D56B1A AC5FB67E55 CAEAB14343 B5F10C0B85 E4673FB5FA AC3AB5DD7B 6376	TrustAsia Global SM2 Root CA G2

Appendix B

Applicable versions of Certification Practice Statement (CPS) and Certificate Policy (CP) in-scope:

Name	Version	Date
TrustAsia Certificate Policy and Certification Practice Statement for SM2 Global Trusted Service	1.1.3	5 February 2024
TrustAsia Certificate Policy and Certification Practice Statement for SM2 Global Trusted Service	1.1.2	26 June 2023

Appendix C

Locations in-scope:

Location	Function
Shanghai (Central), China	Administration and Support
Shanghai (West), China	Datacenter Facility
Shanghai (East), China	Datacenter Facility

MANAGEMENT'S ASSERTION

TrustAsia Technologies, Inc. ("TrustAsia") operates the Certification Authority (CA) services known as CAs in Appendix A, and provides the following CA services:

- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation

The management of TrustAsia 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, and 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 TrustAsia's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

TrustAsia management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in TrustAsia management's opinion, in providing its Certification Authority (CA) services at locations as enumerated in Appendix C, throughout the period 1 August 2023 to 31 July 2024, TrustAsia has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its Certification Practice Statement (CPS) and Certificate Policy (CP) as enumerated in Appendix B
- maintained effective controls to provide reasonable assurance that:
 - TrustAsia's applicable versions of Certification Practice Statement are consistent with its applicable versions of Certificate Policy; and
 - TrustAsia provides its services in accordance with its Certificate Policy and Certification Practice Statement
- 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; and
 - subscriber information is properly authenticated
- maintained effective controls to provide reasonable assurance that:
 - logical and physical access to CA systems and data is restricted to authorised individuals;

- the continuity of key and certificate management operations is maintained; and
- CA systems development, maintenance, and operations are properly authorised 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 and Maintenance
- Business Continuity Management
- Monitoring and Compliance
- Audit Logging

CA Key Lifecycle Management Controls

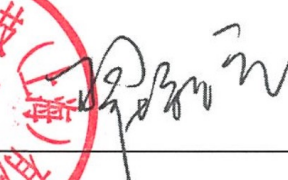
- CA Key Generation
- CA Key Storage, Backup, and Recovery
- CA Public Key Distribution
- CA Key Usage
- CA Key Archival and Destruction
- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management

Certificate Lifecycle Management Controls

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

TrustAsia 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.

After the planned new site within the same city as the main datacenter went into operations during the audit period, TrustAsia had relocated its system resources for production operations from the original data center at Shanghai (East) to the new site at Shanghai (West) and transported all key materials from the original main site to the new site as the new secure location hosting the key materials within the scope. Corresponding controls had been examined for existence and effectiveness physically on site before the new site went into operations and migration conducted for readiness and compliance.



Mr. Xinyuan Zhai

CEO of TrustAsia Technologies, Inc.

32/ F, Building B, No.391, Guiping Road, Xuhui District, Shanghai, China

14 October 2024

Appendix A

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

Subject DN	Key Type	Signature Algorithm	Key Size	Subject Key Identifier	SHA256 Certificate Thumbprints	Certificate Signed by
CN = TrustAsia Global SM2 Root CA G2 OU = GMCA O = TrustAsia Technologies, Inc. C = CN	Root Key	1.2.156.10197. 1.501	256 bits	58A589F8F9F B2659ABF09A 41D6E6E566D 3A539D6	8C18BBBA69 0D957DE6A5 6AE919335F 443431C1D5 8A8634B336 EE239D381A C933	TrustAsia Global SM2 Root CA G2
CN = TrustAsia TLS SM2 CA G2 OU = GMCA O = TrustAsia Technologies, Inc. C = CN	Signing Key	1.2.156.10197. 1.501	256 bits	9DEDDDD76823 81CA1040138 DC9ABC7993E 2DACB3C	4DD45AEF9D 34D2FBABAC E4D52D33BD 7D1F2143C2 CEFD745FF2 31334FF81C C248	TrustAsia Global SM2 Root CA G2
CN = TrustAsia Device SM2 CA G2 OU = GMCA O = TrustAsia Technologies, Inc. C = CN	Signing Key	1.2.156.10197. 1.501	256 bits	D5794D2BD11 9DEA2E5B47B 5CCB4305F0E 967B7B3	2A02C6A634 801162168D 9C6EC2D79A 9D9EB5C67F E2A417CAE5 C2D8A1B73D B70A	TrustAsia Global SM2 Root CA G2
CN = TrustAsia Identity SM2 CA G2 OU = GMCA O = TrustAsia Technologies, Inc. C = CN	Signing Key	1.2.156.10197. 1.501	256 bits	EA67880B3DB 2B54C78516D 3C858599AD2 7F387D2	9F8E2B6EE1 07A27D7F8F 047ABA0E91 BD29A4D6A5 68E0571B4E 7494345A2E FAB1	TrustAsia Global SM2 Root CA G2
CN = DNSPod TLS SM2 CA G2 O = DNSPod, Inc. C = CN	Signing Key	1.2.156.10197. 1.501	256 bits	C27C7F9AB24 47D17B63819 537951D1168 93B6121	AAE8D56B1A AC5FB67E55 CAEAB14343 B5F10C0B85 E4673FB5FA AC3AB5DD7B 6376	TrustAsia Global SM2 Root CA G2

Appendix B

Applicable versions of Certification Practice Statement (CPS) and Certificate Policy (CP) in-scope:

Name	Version	Date
TrustAsia Certificate Policy and Certification Practice Statement for SM2 Global Trusted Service	1.1.3	5 February 2024
TrustAsia Certificate Policy and Certification Practice Statement for SM2 Global Trusted Service	1.1.2	26 June 2023

Appendix C

Locations in-scope:

Location	Function
Shanghai (Central), China	Administration and Support
Shanghai (West), China	Datacenter Facility
Shanghai (East), China	Datacenter Facility

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：亚数信息科技（上海）有限公司管理阶层

我们接受委托，对附件表 A 所列的亚数信息科技（上海）有限公司（TrustAsia Technologies, Inc.，简称“TrustAsia”）于 2023 年 8 月 1 日至 2024 年 7 月 31 日就 TrustAsia 在附件表 C 所列地点运营的电子认证服务其管理阶层认定执行了合理保证的鉴证业务。根据管理阶层认定，TrustAsia 已：

- 于 CP/CPS 中披露了电子认证业务、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
- 通过有效控制机制，以提供以下合理保证：
 - TrustAsia 的 CPS 与 CP 相符；
 - TrustAsia 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；以及
 - 于 TrustAsia 所执行的注册操作恰当地鉴定 SSL 证书申请者的信息
- 通过有效控制机制，以提供以下合理保证：
 - 对 CA 系统和数据的逻辑和物理访问仅限于授权的个人；
 - 保持密钥和证书管理操作的连续性；以及
 - CA 系统的开发，维护和操作得到适当的授权和执行，以维持 CA 系统的完整

以符合 [WebTrust Principles and Criteria for Certification Authorities, v2.2.2](#)。

TrustAsia 未托管其私钥，亦未提供证书挂起服务。据此，我们的程序未延伸至相关标准的有关控制。

于本审计週期，在与主数据中心位于同一城市的新数据中心投入运营后，TrustAsia 已将生产运营的系统资源从原上海（东）数据中心迁移至此上海（西）新数据中心，并将所有密钥材料从原主数据中心运送至新数据中心，以作为审计范围内密钥材料的新安全位置。新数据中心投入运营并进行了迁移前，相应控制措施的存在和有效性已进行了现场检查，以确保准备就绪与合规性。

TrustAsia 的责任

TrustAsia 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 TrustAsia 所提供的服务能够符合 [WebTrust Principles and Criteria for Certification Authorities, v2.2.2](#) 的规定。

审计师的独立性和质量控制

我们保持独立性并遵守国际道德委员会针对会计人员发布的职业会计师道德准则（*Code of Ethics for Professional Accountants*）规定的道德要求，该准则是建立在正直、客观、专业能力和谨慎、保密和职业行为的基本原则之上。

我们公司遵循国际标准要求的品质管理标准（ISQM）1，并据此维护全面的质量控制体系，包括符合道德要求、专业标准和适用法律法规要求的文件化的政策和程序。

审计师的责任

我们的职责是在执行鉴证工作的基础上对 TrustAsia 的管理层认定发表结论。我们根据国际审计与鉴证准则理事会发布的国际鉴证业务准则第 3000 号“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。此准则要求我们计划并执行相应的审计程序以获取所有重大方面和对管理层认定的合理保证，包括：

- (1) 了解 TrustAsia 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) 选择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。

我们相信，我们获取的证据是充分、适当的，为发表鉴证结论提供了基础。

控制的有效性

TrustAsia 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。

固有限制

由于内部控制体系本身的限制，TrustAsia 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。

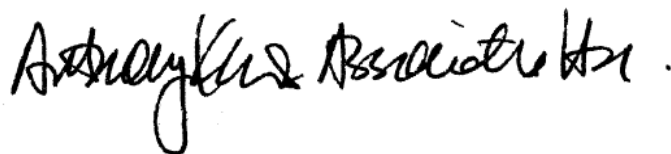
结论

我们认为，TrustAsia 于 2023 年 8 月 1 日至 2024 年 7 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 Principles and Criteria for Certification Authorities, v2.2.2](#)。

本报告并不包括任何在 [WebTrust Principles and Criteria for Certification Authorities, v2.2.2](#) 以外的质量标准声明，或对任何客户对 TrustAsia 服务的合适性声明。

对 Webtrust 标识的使用

在 TrustAsia 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。



Anthony Kam & Associates Ltd.

Certified Public Accountants

2105 Wing On Ctr, 111 Connaught Road, HK SAR, China

14 Oct 2024

KAM Hau Choi Anthony

Practising Certificate Number P02558

附件表 A

本鉴证报告内包括的密钥与证书列举如下:

Subject DN	Key Type	Signature Algorithm	Key Size	Subject Key Identifier	SHA256 Certificate Thumbprints	Certificate Signed by
CN = TrustAsia Global SM2 Root CA G2 OU = GMCA O = TrustAsia Technologies, Inc. C = CN	Root Key	1.2.156.10197. 1.501	256 bits	58A589F8F9F B2659ABF09A 41D6E6E566D 3A539D6	8C18BBBA69 0D957DE6A5 6AE919335F 443431C1D5 8A8634B336 EE239D381A C933	TrustAsia Global SM2 Root CA G2
CN = TrustAsia TLS SM2 CA G2 OU = GMCA O = TrustAsia Technologies, Inc. C = CN	Signing Key	1.2.156.10197. 1.501	256 bits	9DEDDDD76823 81CA1040138 DC9ABC7993E 2DACB3C	4DD45AEF9D 34D2FBABAC E4D52D33BD 7D1F2143C2 CEFD745FF2 31334FF81C C248	TrustAsia Global SM2 Root CA G2
CN = TrustAsia Device SM2 CA G2 OU = GMCA O = TrustAsia Technologies, Inc. C = CN	Signing Key	1.2.156.10197. 1.501	256 bits	D5794D2BD11 9DEA2E5B47B 5CCB4305F0E 967B7B3	2A02C6A634 801162168D 9C6EC2D79A 9D9EB5C67F E2A417CAE5 C2D8A1B73D B70A	TrustAsia Global SM2 Root CA G2
CN = TrustAsia Identity SM2 CA G2 OU = GMCA O = TrustAsia Technologies, Inc. C = CN	Signing Key	1.2.156.10197. 1.501	256 bits	EA67880B3DB 2B54C78516D 3C858599AD2 7F387D2	9F8E2B6EE1 07A27D7F8F 047ABA0E91 BD29A4D6A5 68E0571B4E 7494345A2E FAB1	TrustAsia Global SM2 Root CA G2
CN = DNSPod TLS SM2 CA G2 O = DNSPod, Inc. C = CN	Signing Key	1.2.156.10197. 1.501	256 bits	C27C7F9AB24 47D17B63819 537951D1168 93B6121	AAE8D56B1A AC5FB67E55 CAEAB14343 B5F10C0B85 E4673FB5FA AC3AB5DD7B 6376	TrustAsia Global SM2 Root CA G2

附件表 B

范围内适用之 CP/CPS 版本:

Name	Version	Date
TrustAsia Certificate Policy and Certification Practice Statement for SM2 Global Trusted Service	1.1.3	5 February 2024
TrustAsia Certificate Policy and Certification Practice Statement for SM2 Global Trusted Service	1.1.2	26 June 2023

附件表 C

范围内地点:

Location	Function
Shanghai (Central), China	Administration and Support
Shanghai (West), China	Datacenter Facility
Shanghai (East), China	Datacenter Facility

管理阶层认定报告

(本中文报告只作参考，正文请参阅英文报告)

亚数信息科技 (上海) 有限公司 (以下简称 “TrustAsia”) 运营电子认证服务机构 (以下简称 “CA”)，附件表 A 列举了服务所包括的根证书和中级证书)，并提供以下电子认证服务：

- 订户注册
- 证书更新
- 证书密钥更新
- 证书发布
- 证书分发
- 证书吊销
- 证书验证

TrustAsia 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、以及证书生命周期管理。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 TrustAsia 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。

TrustAsia 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，TrustAsia 管理层认为，于 2023 年 8 月 1 日至 2024 年 7 月 31 日就 TrustAsia 在附件表 C 所列地点提供电子认证服务期间，TrustAsia 已：

- 于附件表 B 之 CP/CPS 中披露了电子认证业务、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
- 通过有效控制机制，以提供以下合理保证：
 - TrustAsia 的 CPS 与 CP 相符；以及
 - TrustAsia 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；以及
 - 于 TrustAsia 所执行的注册操作恰当地鉴定证书申请者的信息；

- 通过有效控制机制，以提供以下合理保证：
 - 对 CA 系统和数据的逻辑和物理访问仅限于授权的个人；
 - 保持密钥和证书管理操作的连续性；以及
 - CA 系统的开发，维护和操作得到适当的授权和执行，以维持 CA 系统的完整；

以符合 [WebTrust Principles and Criteria for Certification Authorities 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
 - 系统开发与维护管理
 - 业务持续性管理
 - 监控与合规管理
 - 审计日志管理
- **CA 密钥生命周期管理**
 - CA 密钥生成
 - CA 密钥存储、备份和恢复
 - CA 公钥分发
 - CA 密钥使用
 - CA 密钥归档和销毁
 - CA 密钥泄露
 - CA 密码设备生命周期管理
- **证书生命周期管理**
 - 订户注册
 - 证书更新

- 证书密钥更新
- 证书发布
- 证书分发
- 证书吊销
- 证书验证

TrustAsia 未托管其私钥，亦未提供证书挂起服务。因此，我们的认定报告未延伸至相关标准的有关控制。

于本审计週期，在与主数据中心位于同一城市的新数据中心投入运营后，TrustAsia 已将生产运营的系统资源从原上海（东）数据中心迁移至此上海（西）新数据中心，并将所有密钥材料从原主数据中心运送至新数据中心，以作为审计范围内密钥材料的新安全位置。新数据中心投入运营并进行了迁移前，相应控制措施的存在和有效性已进行了现场检查，以确保准备就绪与合规性。

总经理 翟新元

亚数信息科技（上海）有限公司
上海市徐汇区桂平路 391 号 B 座 32 层

2024 年 10 月 14 日



附件表 A

本认定报告内包括的密钥与证书列举如下:

Subject DN	Key Type	Signature Algorithm	Key Size	Subject Key Identifier	SHA256 Certificate Thumbprints	Certificate Signed by
CN = TrustAsia Global SM2 Root CA G2 OU = GMCA O = TrustAsia Technologies, Inc. C = CN	Root Key	1.2.156.10197. 1.501	256 bits	58A589F8F9F B2659ABF09A 41D6E6E566D 3A539D6	8C18BBBA69 0D957DE6A5 6AE919335F 443431C1D5 8A8634B336 EE239D381A C933	TrustAsia Global SM2 Root CA G2
CN = TrustAsia TLS SM2 CA G2 OU = GMCA O = TrustAsia Technologies, Inc. C = CN	Signing Key	1.2.156.10197. 1.501	256 bits	9DEDDDD76823 81CA1040138 DC9ABC7993E 2DACB3C	4DD45AEF9D 34D2FBABAC E4D52D33BD 7D1F2143C2 CEFD745FF2 31334FF81C C248	TrustAsia Global SM2 Root CA G2
CN = TrustAsia Device SM2 CA G2 OU = GMCA O = TrustAsia Technologies, Inc. C = CN	Signing Key	1.2.156.10197. 1.501	256 bits	D5794D2BD11 9DEA2E5B47B 5CCB4305F0E 967B7B3	2A02C6A634 801162168D 9C6EC2D79A 9D9EB5C67F E2A417CAE5 C2D8A1B73D B70A	TrustAsia Global SM2 Root CA G2
CN = TrustAsia Identity SM2 CA G2 OU = GMCA O = TrustAsia Technologies, Inc. C = CN	Signing Key	1.2.156.10197. 1.501	256 bits	EA67880B3DB 2B54C78516D 3C858599AD2 7F387D2	9F8E2B6EE1 07A27D7F8F 047ABA0E91 BD29A4D6A5 68E0571B4E 7494345A2E FAB1	TrustAsia Global SM2 Root CA G2
CN = DNSPod TLS SM2 CA G2 O = DNSPod, Inc. C = CN	Signing Key	1.2.156.10197. 1.501	256 bits	C27C7F9AB24 47D17B63819 537951D1168 93B6121	AAE8D56B1A AC5FB67E55 CAEAB14343 B5F10C0B85 E4673FB5FA AC3AB5DD7B 6376	TrustAsia Global SM2 Root CA G2

附件表 B

范围内适用之 CP/CPS 版本:

Name	Version	Date
TrustAsia Certificate Policy and Certification Practice Statement for SM2 Global Trusted Service	1.1.3	5 February 2024
TrustAsia Certificate Policy and Certification Practice Statement for SM2 Global Trusted Service	1.1.2	26 June 2023

附件表 C

范围内地点:

地点	功能
中国上海(中)	管理与支持
中国上海(西)	数据中心
中国上海(东)	数据中心