

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 S/MIME certificate life cycle management business practices in its Certification Practice Statement (CPS) and Certificate Policy (CP) as enumerated in Appendix B, including its commitment to provide S/MIME certificates in conformity with the CA/Browser Forum Requirements on the TrustAsia website, and provided such services in accordance with its disclosed practices
- maintained effective controls to provide reasonable assurance that:
 - the integrity of keys and S/MIME certificates it manages is established and protected throughout their lifecycles; and
 - S/MIME certificate 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 – S/MIME, v1.0.3](#).

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 – S/MIME, v1.0.3](#).

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 S/MIME certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of S/MIME certificates;
- (2) selectively testing transactions executed in accordance with disclosed S/MIME certificate lifecycle management business practices;
- (3) testing and evaluating the operating effectiveness of the controls; and
- (4) performing such other procedures as we considered necessary in the circumstances.

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 – S/MIME, v1.0.3](#).

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 – S/MIME, v1.0.3](#), 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 – S/MIME Certificates Seal constitutes a symbolic

AKAM


2105 Wing On Ctr, 111 Connaught Rd, HK

Anthony KAM
& associates ltd
certified public accountants
爾孝財會計師行有限公司

+852 2246 6888

info@akamcpa.com

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 Secure Email RSA CA O = TrustAsia Technologies, Inc. C = CN	Signing Key	Sha256RSA	4096 bits	FCB3E33D448 455D2FF172D 1C4DF961090 3C6D94A	E67767E9C7 2E0691497F 66616590D9 9AFDC60974 FE6F1F4F1B FD71B2A13E 2C03	TrustAsia Global Root CA G1
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 Secure Email RSA CA G3 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	EB164C7D748 A091C5787C3 5B9B98FF213 6C3B20A	C84E9EE522 5DF7B674A5 7343C6D489 21907E9764 010042E40B 2C00F94463 9CA4	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	BE4B56CB50 56C0136A52 6DF444508D AA36A0B54F 42E4AC38F7 2AF470E479 654C	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	70342F6C5E 0FD9F9ABE3 C1448D033E 1A0CAB4CC5 60409E1C03 B626E48B8B 16DD	TrustAsia Global Root CA G4
CN = TrustAsia SMIME RSA Root CA O = TrustAsia Technologies, Inc. C = CN	Root Key	sha384RSA	4096 bits	801AAA43C1C 97F8B1A9645 BC3DBB6B485 26C5BAB	C7796BEB62 C101BB143D 262A7C96A0 C616818322 3EF50D6996 32D86E03B8 CC9B	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	BC2197C0C1 FF17C55337 0BF9955B9B 50C8C9D27A 0C28F78704 E00C881F14 58AA	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	436472C100 9A325C54F1 A5BBB5468A 7BAEECCBE0 5DE5F099CB 70D3FE41E1 3C16	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	E21C0762F0 B1777AB2B0 6E9F9273BE 251AB9FBB3 D5DD901F60 750EF9B53B 8488	TrustAsia SMIME 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 S/MIME CA services.

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

There are inherent limitations in any controls, including the possibility of human error, and the circumvention or overriding of controls. Accordingly, even effective controls can only provide reasonable assurance with respect to 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 S/MIME CA services. Based on that assessment, in TrustAsia management's opinion, in providing its S/MIME CA services at locations as enumerated in Appendix C, throughout the period 1 August 2023 to 31 July 2024, TrustAsia has:

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

in accordance with the [WebTrust Principles and Criteria for Certification Authorities – S/MIME – Version 1.0.3](#).

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 Root CA G1 O = TrustAsia Technologies, Inc. C = CN	Root Key	Sha256RSA	4096 bits	24C20F2CCDC0B5154F6B6DD4F2F058FE1443DFF4	05F82DE4B4A9ED4B7CD1F3ACE9B73BD6DB69D87816DD3847195CF737ED2951E7	TrustAsia Global Root CA G1
CN = TrustAsia Secure Email RSA CA O = TrustAsia Technologies, Inc. C = CN	Signing Key	Sha256RSA	4096 bits	FCB3E33D448455D2FF172D1C4DF9610903C6D94A	E67767E9C72E0691497F66616590D99AFDC60974FE6F1F4F1BFD71B2A13E2C03	TrustAsia Global Root CA G1
CN = TrustAsia Global Root CA G3 O = TrustAsia Technologies, Inc. C = CN	Root Key	sha384RSA	4096 bits	40E4E4F223EF38CAB0AE577FF221301634DBBC92	E0D3226AEB1163C2E48FF9BE3B50B4C6431BE7BB1EACC5C36B5D5EC509039A08	TrustAsia Global Root CA G3
CN = TrustAsia Secure Email RSA CA G3 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	EB164C7D748A091C5787C35B9B98FF2136C3B20A	C84E9EE5225DF7B674A57343C6D48921907E9764010042E40B2C00F944639CA4	TrustAsia Global Root CA G3
CN = TrustAsia Global Root CA G4 O = TrustAsia Technologies, Inc. C = CN	Root Key	sha384ECDSA	384 bits	A5BB4A97CEB32B7FA431DE97835983A66F71CBDE	BE4B56CB5056C0136A526DF444508DAA36A0B54F42E4AC38F72AF470E479654C	TrustAsia Global Root CA G4
CN = TrustAsia Secure Email ECC CA G4 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384ECDSA	384 bits	613250574BF3266AE9C8D7C61337F17E1553B3AC	70342F6C5E0FD9F9ABE3C1448D033E1A0CAB4CC560409E1C03B626E48B8B16DD	TrustAsia Global Root CA G4
CN = TrustAsia SMIME RSA Root CA O = TrustAsia Technologies, Inc. C = CN	Root Key	sha384RSA	4096 bits	801AAA43C1C97F8B1A9645BC3DBB6B48526C5BAB	C7796BEB62C101BB143D262A7C96A0C6168183223EF50D699632D86E03B8CC9B	TrustAsia SMIME RSA Root CA
CN = TrustAsia SMIME RSA CA 2024 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	20741B3D5325D2968E28468167E43DB50550784B	BC2197C0C1FF17C553370BF9955B9B50C8C9D27A0C28F78704E00C881F1458AA	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	436472C100 9A325C54F1 A5BBB5468A 7BAEECCBE0 5DE5F099CB 70D3FE41E1 3C16	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	E21C0762F0 B1777AB2B0 6E9F9273BE 251AB9FBB3 D5DD901F60 750EF9B53B 8488	TrustAsia SMIME 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

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 日期间于附件表 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：

- 于附件表 B 的 CP/CPS 中披露了 S/MIME 证书生命周期业务规则，包括承诺遵循 CA/Browser 论坛的相关指引提供 S/MIME 证书服务，并依据披露的业务规则提供相关服务
- 通过有效控制机制，以提供以下合理保证：
 - 建立并保护所管理的密钥和 S/MIME 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 S/MIME 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 – S/MIME, v1.0.3](#)。

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 – S/MIME, v1.0.3](#) 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 S/MIME 证书生命周期管理，包括 S/MIME 证书发放、更新和吊销；
- (2) 选择测试业务操作是否遵守了所披露的 S/MIME 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。

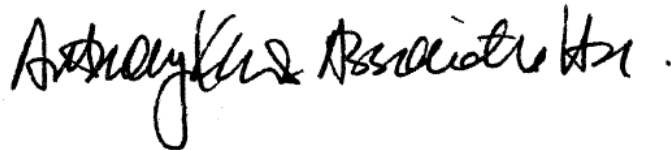
结论

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阶层认定在所有重大方面符合 [WebTrust Principles and Criteria for Certification Authorities – S/MIME, v1.0.3](#)。

本报告并不包括任何在 [WebTrust Principles and Criteria for Certification Authorities – S/MIME, v1.0.3](#) 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 S/MIME 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	24C20F2CCDC 0B5154F6B6D D4F2F058FE1 443DFF4	05F82DE4B4 A9ED4B7CD1 F3ACE9B73B D6DB69D878 16DD384719 5CF737ED29 51E7	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	E67767E9C7 2E0691497F 66616590D9 9AFDC6097A FE6F1F4F1B FD71B2A13E 2C03	TrustAsia Global Root CA G1
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 Secure Email RSA CA G3 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	EB164C7D748 A091C5787C3 5B9B98FF213 6C3B20A	C84E9EE522 5DF7B674A5 7343C6D489 21907E9764 010042E40B 2C00F94463 9CA4	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	BE4B56CB50 56C0136A52 6DF444508D AA36A0B54F 42E4AC38F7 2AF470E479 654C	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	70342F6C5E 0FD9F9ABE3 C1448D033E 1A0CAB4CC5 60409E1C03 B626E48B8B 16DD	TrustAsia Global Root CA G4
CN = TrustAsia SMIME RSA Root CA O = TrustAsia Technologies, Inc. C = CN	Root Key	sha384RSA	4096 bits	801AAA43C1C 97F8B1A9645 BC3DDB6B485 26C5BAB	C7796BEB62 C101BB143D 262A7C96A0 C616818322 3EF50D6996 32D86E03B8 CC9B	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	BC2197C0C1 FF17C55337 0BF9955B9B 50C8C9D27A 0C28F78704 E00C881F14 58AA	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	436472C100 9A325C54F1 A5BBB5468A 7BAEECCBE0 5DE5F099CB 70D3FE41E1 3C16	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	E21C0762F0 B1777AB2B0 6E9F9273BE 251AB9FBB3 D5DD901F60 750EF9B53B 8488	TrustAsia SMIME 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 CA 所包括的根证书和中级证书），并提供 S/MIME 电子认证服务。

TrustAsia 的管理层负责针对 S/MIME CA 服务建立并维护有效的控制，包括：S/MIME CA 业务规则披露、S/MIME CA 业务规则管理、S/MIME CA 密钥生命周期管理、以及 S/MIME 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 S/MIME 电子认证服务期间，TrustAsia 已：

- 在附件表 B 之 CP/CPS 中披露了 S/MIME 证书生命周期业务规则，包括承诺遵循 CA/Browser 论坛的相关指引提供 S/MIME 证书服务，并依据披露的业务规则提供相关服务
- 通过有效控制机制，以提供以下合理保证：
 - 建立并保护所管理的密钥和 S/MIME 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 S/MIME 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 – S/MIME – Version 1.0.3](#)。

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 Secure Email RSA CA O = TrustAsia Technologies, Inc. C = CN	Signing Key	Sha256RSA	4096 bits	FCB3E33D448 455D2FF172D 1C4DF961090 3C6D94A	E67767E9C7 2E0691497F 66616590D9 9AFDC60974 FE6F1F4F1B FD71B2A13E 2C03	TrustAsia Global Root CA G1
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 Secure Email RSA CA G3 O = TrustAsia Technologies, Inc. C = CN	Signing Key	sha384RSA	4096 bits	EB164C7D748 A091C5787C3 5B9B98FF213 6C3B20A	C84E9EE522 5DF7B674A5 7343C6D489 21907E9764 010042E40B 2C00F94463 9CA4	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	BE4B56CB50 56C0136A52 6DF444508D AA36A0B54F 42E4AC38F7 2AF470E479 654C	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	70342F6C5E 0FD9F9ABE3 C1448D033E 1A0CAB4CC5 60409E1C03 B626E48B8B 16DD	TrustAsia Global Root CA G4
CN = TrustAsia SMIME RSA Root CA O = TrustAsia Technologies, Inc. C = CN	Root Key	sha384RSA	4096 bits	801AAA43C1C 97F8B1A9645 BC3DBB6B485 26C5BAB	C7796BEB62 C101BB143D 262A7C96A0 C616818322 3EF50D6996 32D86E03B8 CC9B	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	BC2197C0C1 FF17C55337 0BF9955B9B 50C8C9D27A 0C28F78704 E00C881F14 58AA	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	436472C100 9A325C54F1 A5BBB5468A 7BAEECCBE0 5DE5F099CB 70D3FE41E1 3C16	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	E21C0762F0 B1777AB2B0 6E9F9273BE 251AB9FBB3 D5DD901F60 750EF9B53B 8488	TrustAsia SMIME 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