

INDEPENDENT ASSURANCE REPORT

To the management of *Aspire Technologies (Shenzhen) Ltd.* ("CMCA")

Scope

We have been engaged, in a reasonable assurance engagement, to report on CMCA management's assertion that for its Certification Authority (CA) operations at Guangzhou and Changsha, China, throughout the period 28 January 2021 to 27 January 2022 as enumerated in [Attachment A](#), CMCA has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
 - [Certification Practice Statement Version 1.0.1 August 2021](#)
 - [Certification Practice Statement Version 0.2 October 2020](#)
- maintained effective controls to provide reasonable assurance that
 - CMCA provides its services in accordance with its Certification Practice Statements
- maintained effective controls to provide reasonable assurance that:
 - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
 - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles;
 - subscriber information is properly authenticated (for the registration activities performed by CMCA); and
 - subordinate CA certificate requests are accurate, authenticated, and approved
- maintained effective controls to provide reasonable assurance that:
 - logical and physical access to CA systems and data is restricted to 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 service Principles and Criteria for Certification Authorities Version 2.2.1](#).

CMCA does not escrow its CA keys, does not provide subscriber key generation services and certificate suspension services, and does not issue subordinate CA or cross certificates to non-affiliated CAs. Accordingly, our procedures did not extend to controls that would address those criteria.

Certification authority's responsibilities

CMCA'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 v2.2.1.

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.

We apply International Standard on Quality Control 1, and accordingly maintain 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

It is our responsibility to express an opinion on the management's assertion based on our work performed and to report our opinion solely to you, in accordance with our agreed terms of engagement and for no other purpose. We do not assume responsibility towards or accept liability to any other person for the contents of this report.

We conducted our work in accordance with International Standard on Assurance Engagements 3000 Revised, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, 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 CMCA'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 CMCA 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, CMCA's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorised access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any 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 28 January 2021 to 27 January 2022, CMCA 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 v2.2.1.

This report does not include any representation as to the quality of CMCA's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities v2.2.1, nor the suitability of any of CMCA's services for any customer's intended purpose.

Use of the WebTrust seal

If a seal is issued CMCA'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.

A handwritten signature in cursive script that reads "Deloitte Touche Tohmatsu".

Deloitte Touche Tohmatsu
Hong Kong
20 April 2022

ATTACHMENT A

LIST OF IN SCOPE CAs

Root CAs
1. CMCA GLOBAL TRUST ROOT CA
Issuing CAs
2. CMCA EV SSL CA
3. CMCA SSL CA

CA IDENTIFYING INFORMATION

CA#	Cert#	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
1	1	CN = CMCA GLOBAL TRUST ROOT CA O = Aspire Technologies C = CN	CN = CMCA GLOBAL TRUST ROOT CA O = Aspire Technologies C = CN	00BF7A BDC8E5 F69594 F413B1 9D	rsaEncryption	4096 bits	sha256WithR SAEncryption	16 October 2020 15:38:1 7	16 October 2045 15:38:17	B795CD0 18EE5743 51E6A0A D38C7AE 6367976 170C	1108210FCE22F535 F274B4733A1E055 0E68405D5381DCE D95B864D9AF53D0 B69
2	1	CN = CMCA SSL CA O = Aspire Technologies C = CN	CN = CMCA GLOBAL TRUST ROOT CA O = Aspire Technologies C = CN	00AD4E 06AB7F 624426 C14746 2D	rsaEncryption	4096 bits	sha256WithR SAEncryption	16 October 2020 16:30:2 4	16 October 2040 16:30:24	D240F9E 29CAA72 BA48F0E 93B5998 1644388 D51CD	C5DA1616FD4168E 9444FFE50C37BA9 C3989E18AADF146 4C7B2341D10235B 375E
3	1	CN = CMCA EV SSL CA O = Aspire Technologies C = CN	CN = CMCA GLOBAL TRUST ROOT CA O = Aspire Technologies C = CN	00D571 AB1B6A C699AE FD360D B3	rsaEncryption	4096 bits	sha256WithR SAEncryption	16 October 2020 16:35:3 2	16 October 2040 16:35:32	16451C7 F35E91B 60613AA 994F7232 EBD9007 C4F2	0D7314BC565EF94 BFEC133D3B58E8C 447940AF76FECAE 4B0468E4D0DF60A 7014

CMCA MANAGEMENT'S ASSERTION

Assertion by Management of Aspire Technologies (Shenzhen) Ltd. regarding its Disclosure of its Business Practices and its Controls Over its Certification Authority Operations during the period from January 28, 2021 through January 27, 2022.

Aspire Technologies (Shenzhen) Ltd. operates as a Certification Authority ("CMCA") services as enumerated in [Attachment A](#) and provides the follow CA services:

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

The management of CMCA 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 controls. Accordingly, even effective internal controls can only provide only reasonable assurance with respect to CMCA's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

Aspire Technologies (Shenzhen) Ltd. ("CMCA") management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in CMCA management's opinion, in providing its Certification Authority (CA) services at Guangzhou and Changsha, China, throughout the period January 28, 2021 to January 27, 2022, CMCA has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
 - [Certification Practice Statement Version 1.0.1 August 2021](#)
 - [Certification Practice Statement Version 0.2 October 2020](#)
- maintained effective controls to provide reasonable assurance that CMCA provides its services in accordance with its Certification Practice Statements
- maintained effective controls to provide reasonable assurance that:
 - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
 - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles;
 - subscriber information was properly authenticated (for the registration activities performed by CMCA); and
 - subordinate CA certificate requests are accurate, authenticated, and approved;
- maintained effective controls to provide reasonable assurance that:
 - logical and physical access to CA systems and data is restricted to authorized individuals;
 - the continuity of key and certificate lifecycle management operations was maintained; and

- CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity

in accordance with the [WebTrust service Principles and Criteria for Certification Authorities Version 2.2.1](#), including the following:

CA Business Practices Disclosure

- Certification Practice Statement (CPS)
- Certificate Policy (CP)

CA Business Practices Management

- Certification Practice Statement Management
- Certificate Policy 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, and Change Management
- Disaster Recovery, Backups, and Business Continuity Management
- Monitoring and Compliance
- Audit Logging

CA Key Lifecycle Management Controls

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

Certificate Lifecycle Management Controls

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

CMCA does not escrow its CA keys, does not provide subscriber key generation services and certificate suspension services, and does not issue subordinate CA or cross certificates to non-affiliated CAs. Accordingly, our assertion does not extend to controls that would address those criteria.

[CMCA Representative]



[Title of the representative]

霍世峰

**ATTACHMENT A
LIST OF IN SCOPE CAs**

Root CAs
1. CMCA GLOBAL TRUST ROOT CA
Issuing CAs
2. CMCA EV SSL CA
3. CMCA SSL CA

CA IDENTIFYING INFORMATION

CA#	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
1	1	CN = CMCA GLOBAL TRUST ROOT CA O = Aspire Technologies C = CN	CN = CMCA GLOBAL TRUST ROOT CA O = Aspire Technologies C = CN	00BF7A BDC8E5 F69594 F413B1 9D	rsaEncryption	4096 bits	sha256WithR SAEncryption	16 October 2020 15:38:17	16 October 2045 15:38:17	B795CD0 18EE5743 51E6A0A D38C7AE 6367976 170C	1108210FCE22F5 35F274B4733A1E 0550E68405D538 1DCED95B864D9 AF53D0B69
2	1	CN = CMCA SSL CA O = Aspire Technologies C = CN	CN = CMCA GLOBAL TRUST ROOT CA O = Aspire Technologies C = CN	00AD4E 06AB7F 624426 C14746 2D	rsaEncryption	4096 bits	sha256WithR SAEncryption	16 October 2020 16:30:24	16 October 2040 16:30:24	D240F9E 29CAA72 BA48F0E 93B5998 1644388 D51CD	C5DA1616FD416 8E9444FFE50C37 BA9C3989E18AA DF1464C7B2341 D10235B375E
3	1	CN = CMCA EV SSL CA O = Aspire Technologies C = CN	CN = CMCA GLOBAL TRUST ROOT CA O = Aspire Technologies C = CN	00D571 AB1B6A C699AE FD360D B3	rsaEncryption	4096 bits	sha256WithR SAEncryption	16 October 2020 16:35:32	16 October 2040 16:35:32	16451C7 F35E91B 60613AA 994F7232 EBD9007 C4F2	0D7314BC565EF9 4BFEC133D3B58E 8C447940AF76FE CAE4B0468E4D0 DF60A7014