



Baker Tilly MH Consulting Sdn Bhd
(1068792-P)
C-10-07, Sunway Nexis
No.1, Jalan PJU 5/1, Kota Damansara
47810 Petaling Jaya, Selangor, Malaysia

T: +603 6145 0889
F: +603 6158 9923
M: +6012 620 9868

info@bakertillyconsulting.com.my
www.bakertilly.my

Independent Assurance Report

To the Board of Raffcomm Technologies Sdn Bhd:

Scope

We have been engaged, in reasonable assurance engagement, to report on Raffcomm Technologies Sdn Bhd Management's Assertion that for its Certification Authority operations, known as RAFFTECH-CA, at the following locations:

- Business Operations: Kuala Lumpur, Wilayah Persekutuan Kuala Lumpur, Malaysia
- Primary Data Centre: Cyberjaya, Selangor, Malaysia
- Disaster Recovery Centre: Kuala Lumpur, Wilayah Persekutuan Kuala Lumpur, Malaysia

Throughout the period 19 February 2022 to 18 February 2023, for its CAs as enumerated in [Appendix 1 – List of Root and Subordinate CAs in Scope](#), RAFFTECH-CA has:

- Disclosed its business, key and certification life cycle management business and CA environmental practices in its:
 - [RAFFTECH-CA Certificate Policy \(CP\) Version 1.3 dated 18 February 2023](#)
 - [RAFFTECH-CA Certification Practice Statement \(CPS\) Version 1.3 dated 18 February 2023](#)
- Suitably designed and placed into operation controls to provide reasonable assurance that:
 - RAFFTECH-CA Certification Practice Statement is consistent with RAFFTECH-CA Certificate Policy.
 - RAFFTECH-CA provides its services in accordance with its Certificate Policy and Certification Practice Statement.
- Suitably designed and placed into operation controls to provide reasonable assurance that:
 - The integrity of keys and certificates it manages are established and protected throughout their lifecycles.
 - The integrity of subscriber keys and certificates it manages are established and protected throughout their lifecycles.
 - Subscriber information is properly authenticated for the registration activities performed by RAFFTECH-CA.

- Subordinate CA certificate requests are accurate, authenticated, and approved.
- Suitably designed and placed into operation 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.
 - 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 Version 2.2.2](#).

Our examination was conducted in accordance with attestation standards by Chartered Professional Accountants Canada (“CPA Canada”) [WebTrust Principles and Criteria for Certification Authorities Version 2.2.2](#).

RAFFTECH-CA makes use of external registration authorities for specific subscriber registration activities. Our examination did not extend to the controls exercised by these external registration authorities.

RAFFTECH-CA does not escrow and migrate its CA key, does not provide subscriber’s key archival, destruction and escrow services, does not provide certificate rekey and suspension services, does not use Integrated Circuit Card (“ICC”), does not practice subordinate CA cross-certification. Accordingly, our assertion does not extend to controls that would address those criteria.

Certification authority’s responsibility

The Board and Management of RAFFTECH-CA are responsible for their 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 Version 2.2.2](#).

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 behavior.

We have applied 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.

Practitioner’s responsibilities

Our responsibility is to express an opinion on management’s assertion¹⁶ 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:

- Obtaining an understanding of RAFFTECH-CA’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.
- Selectively testing transactions executed in accordance with disclosed key and certificate lifecycle management business practices.
- Testing and evaluating the operating effectiveness of the controls.

- 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.

The relative effectiveness and significance of specific controls at RAFFTECH-CA 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.

Suitability of controls

The suitability of the design of the controls at RAFFTECH-CA 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 suitability of the design of the controls at individual subscriber and relying party locations.

Inherent limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. For example, because of their nature, controls may not prevent, or detect unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection to the future of any conclusions based on our findings is subject to the risk that controls may become ineffective.

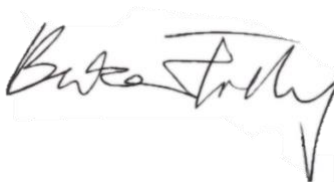
Opinion

In our opinion, from 19 February 2022 to 18 February 2023, RAFFTECH-CA's Management Assertion is fairly stated, in all material respects, in accordance with the [WebTrust Principles and Criteria for Certification Authorities Version 2.2.2.](#)

This report does not include any representation as to the quality of RAFFTECH-CA's services beyond those covered by the [WebTrust Principles and Criteria for Certification Authorities Version 2.2.2.](#), nor the suitability of any of RAFFTECH-CA's services for any customer's intended purpose.

Use of the WebTrust seal

RAFFTECH-CA'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.



Baker Tilly MH Consulting Sdn Bhd
Kuala Lumpur, Malaysia
27 May 2023



RAFFTECH-CA Management's Assertion

Raffcomm Technologies Sdn. Bhd. (RAFFTECH-CA) operates the Certification Authority ("CA") services, as referred to in [Appendix 1 – List of Root CA and Subordinate CAs](#) and provides the following CA services:

- Subscriber registration
- Certificate renewal
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation
- Subscriber key generation and management

The management of RAFFTECH-CA is responsible for establishing and maintaining effective controls over its CA operations, including CA business practices disclosure, on its RAFFTECH- CA Repository at www.rafftech.my/wp/knowledge. These controls contain monitoring mechanism and actions are taken to correct deficiencies identified.

The management of RAFFTECH-CA has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in RAFFTECH-CA management's opinion, in providing its Certification Authority (CA) services at the following locations:

- Business Operations: Kuala Lumpur, Wilayah Persekutuan Kuala Lumpur, Malaysia
- Primary Data Centre: Cyberjaya, Selangor, Malaysia
- Disaster Recovery Centre: Kuala Lumpur, Wilayah Persekutuan Kuala Lumpur, Malaysia

Throughout the period of 9 February 2022 to 18 February 2023, RAFFTECH-CA has disclosed its business, key and certification life cycle management business and CA environmental practices in its:

- [RAFFTECH-CA Certificate Policy \(CP\) Version 1.3 dated 18 February 2023](#)
- [RAFFTECH-CA Certification Practice Statement \(CPS\) Version 1.3 dated 18 February 2023](#)

Suitably designed and placed into operation controls to provide reasonable assurance that:

- RAFFTECH-CA Certification Practice Statement is consistent with RAFFTECH-CA Certificate Policy.
- RAFFTECH-CA provides its services in accordance with its Certificate Policy and Certification Practice Statement.

Suitably designed and placed into operation 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 RAFFTECH-CA.
- Subordinate CA certificate requests are accurate, authenticated and approved.

Suitably designed and placed into operation 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.
- 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 Version 2.2.2](#) including the following:

CA Business Practices Disclosure

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

CA Business Practices Management

- Certification 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, 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 and Destruction
- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management
- CA Key Transportation

Subscriber Key Lifecycle Management Controls

- CA-Provided Subscriber Key Generation Services
- CA-Provided Subscriber Storage and Recovery Services
- Requirement for Subscriber Key Management

Certificate Lifecycle Management Controls

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

Subordinate CA Certificate Lifecycle Management Controls

- Subordinate CA Certificate Lifecycle Management

RAFFTECH-CA does not escrow and migrate its CA key, does not provide subscriber's key archival, destruction and escrow services, does not provide certificate rekey and suspension services, does not use Integrated Circuit Card ("ICC"), does not practice subordinate CA cross-certification. Accordingly, our assertion does not extend to controls that would address those criteria.



Mohamed Niza Abu Bakar
Group Chief Executive Officer
On Behalf of the Board and Management of Raffcomm Technologies Sdn Bhd
27 May 2023

Appendix 1 – List of Root and Subordinate CAs In Scope

| |
|---|
| 1. CypherSign Class 1 Root CA |
| 1.1 CypherSign Personal |
| 2. CypherSign Class 2 Root CA |
| 2.1 CypherSign Pro 2.2 CypherSign Organizational 2.3 Rafftech Time Stamping Authority |
| 3. RAFFTECH Class 2 ECC Root CA |
| 3.1 GPKI CA ECC |
| 4. RAFFTECH Class 2 RSA Root CA |
| 4.1 GPKI CA RSA |

Appendix 2 – Identifying Information for CAs In Scope

| CA | Subject DN | Issuer DN | Serial | Key Algorithm | Key Size (bits) | Digest Algorithm | Issuance Date | Expiration Date | Subject Key Identifier | Fingerprint SHA-256 |
|-----|---|--|--------------------------|---------------|-----------------|-------------------|----------------------------------|----------------------------------|---|--|
| 1 | CN=CypherSign Class 1 Root CA, O=Raffcomm Technologies Sdn Bhd, C=MY | CN=CypherSign Class 1 Root CA, O=Raffcomm Technologies Sdn Bhd, C=MY | 532582 6DC2FE B505 | RSA | 4096 | SHA512W ITHRSA | 2018-01-11 14:52:09 +08:00 | 2043-01-05 14:52:09 +08:00 | 8E 83 91 67 EA 5BBD 4B BA59 49 C43D 8C 62 91 0F 95 33 0F | F3 61 53 75 3B F673 50 C5 32 F2 E3F8 EE CDA5 26 25F6 E7 87 A8 DD DDA4 98 D2 91 B2 A67D 12 |
| 1.1 | CN=CypherSign Personal, OU=1000449-W, O=Raffcomm Technologies Sdn Bhd, C=MY | CN=CypherSign Class 1 Root CA, O=Raffcomm Technologies Sdn Bhd, C=MY | 5EF48F EEF16E 79C1 | RSA | 2048 | SHA256W ITHRSA | 2018-01-11 15:32:05 +08:00 | 2028-01-09 15:32:05 +08:00 | 81 1F 82 21 5C A3 60 4E D3 22 AE 5847 F9 5969 24 81DB A0 | E0 C4 892A B6 3FFA 32 56 63 50 1C 5F 4F 55 8C 9D 6B 5D 37 6E 24 28 34 9D 0C 69 9C 66 BBA0 1B |

| CA | Subject DN | Issuer DN | Serial | Key Algorithm | Key Size (bits) | Digest Algorithm | Issuance Date | Expiration Date | Subject Key Identifier | Fingerprint SHA-256 |
|-----|---|--|------------------|---------------|-----------------|-------------------|----------------------------|----------------------------|---|---|
| 2 | CN=CypherSign Class 2 Root CA, O=Raffcomm Technologies Sdn Bhd, C=MY | CN=CypherSign Class 2 Root CA, O=Raffcomm Technologies Sdn Bhd, C=MY | 674B83560669C3C9 | RSA | 4096 | SHA512W ITHRSA | 2018-01-11 14:55:53 +08:00 | 2043-01-05 14:55:53 +08:00 | 25 F7 D9 64 8E 4A 79 FC 4DCD E5 93CA 86 6AFD DE 2F 21 73 | 4F 95 60B4 E8 F1 53 61 CAF7 04 E860 57 630E AC FF E8 83 B9C0 C8 8237 F7 63CA 02 0A 3A C6 |
| 2.1 | CN=CypherSign Pro, OU=1000449-W, O=Raffcomm Technologies SdnBhd, C=MY | CN=CypherSign Class 2 Root CA, O=Raffcomm Technologies Sdn Bhd, C=MY | 79F0C3447FE6228B | RSA | 2048 | SHA256W ITHRSA | 2018-01-11 15:35:37 +08:00 | 2028-01-09 15:35:37 +08:00 | 9B A6 81A5 3C F4FB BC 79 79 BC B23E A5 054F 2E 2183 69 | 6D 0F CE E1 37 0F EA 88 47 BA F8 785A DD 5B 2D 10 FF 90 1A 51 1D 89 13 2A FA A1 25 CC 64E8 43 |
| 2.2 | CN=CypherSign Organizational, OU=1000449-W, O=Raffcomm Technologies Sdn Bhd, C=MY | CN=CypherSign Class 2 Root CA, O=Raffcomm Technologies Sdn Bhd, C=MY | 7EDE095425A7905E | RSA | 2048 | SHA512W ITHRSA | 2018-01-11 15:39:13 +08:00 | 2028-01-09 15:39:13 +08:00 | 32 36 F6 30 B4 CB1B 98 408A 98 162C 42 F9 DE 90 7ADB C8 | F7 1E 2E 94 D6 06 44 3D 1D 37 6E 3CBC 21 9807 EA B4B0 AB BD DF A4 26C1 B9 B66B D8 5F6D 7C |

| CA | Subject DN | Issuer DN | Serial | Key Algorithm | Key Size (bits) | Digest Algorithm | Issuance Date | Expiration Date | Subject Key Identifier | Fingerprint SHA-256 |
|-----|---|--|--------------------|---------------|-----------------|-------------------------|----------------------------------|----------------------------------|---|---|
| 2.3 | CN=Rafftech Time Stamping Authority, OU=1000449- W, O=Raffcomm Technologies Sdn Bhd, C=MY | CN=CypherSign Class 2 Root CA, O=Raffcomm Technologies Sdn Bhd, C=MY | 30ABAC D3820E 324A | RSA | 2048 | SHA256W ITHRS A | 2019-04-29 15:55:46 +08:00 | 2029-04-26 15:55:46 +08:00 | 5A 7D CFB9 09 8DDD 9F D6 31 BF B437 46 A53A 4D 1E20 74 | 56 26 89 21 3F 4EC3 C9 EAF1 C7 14D7 C5 61 24 8D 07A5 65 B34B 43 E17A B3 78 2B F4 3F54 13 |
| 3 | CN=RAFFTECH Class 2 ECC Root CA, O=Raffcomm Technologies SdnBhd, C=MY | CN=RAFFTECH Class 2 ECC Root CA, O=Raffcomm Technologies Sdn Bhd, C=MY | 605BAF 7812EA 114B | EC | 384 | SHA384W ITHECDS A | 2021-03-10 11:16:19 +08:00 | 2046-03-04 11:16:19 +08:00 | 26 C0 5CFF D2 174C BA 767D 5F EA 8A 7B 2D02 C0 A31E 1E | 6E D7 3C 5F 47 DC 10 6E 83 8B 97 F8 FA 61 1A 11 E0 71 5A E4 08CD B3 3F7C 52 85D7 F2 1B 12 43 |

| CA | Subject DN | Issuer DN | Serial | Key Algorithm | Key Size (bits) | Digest Algorithm | Issuance Date | Expiration Date | Subject Key Identifier | Fingerprint SHA-256 |
|-----|--|--|--------------------------|---------------|-----------------|-------------------------|----------------------------------|----------------------------------|---|---|
| 3.1 | CN=GPKI CA ECC, OU=MAMPU, O=Raffcomm Technologies Sdn Bhd, L=Putrajaya, ST=Wilayah Persekutuan, C=MY | CN=RAFFTECH Class 2 ECC Root CA, O=Raffcomm Technologies Sdn Bhd, C=MY | 4987CE 4DB005 4C2C | EC | 384 | SHA384W ITHECDS A | 2021-03-10 11:48:12 +08:00 | 2031-03-08 11:48:12 +08:00 | CA BE E6E4 39 56 4C EB 13 64 7F 1B56 40 3E8C D4 B0E6 4C | F0 11 AF 9E 63 C3 B0 2B 91 B9 81 9C6A 3A DEE5 88 7B 69 EA 124A B4 40CD 20 2FA4 99 7D 2A 56 |
| 4 | CN=RAFFTECH Class 2 RSA Root CA, O=Raffcomm Technologies SdnBhd, C=MY | CN=RAFFTECH Class 2 RSA Root CA, O=Raffcomm Technologies Sdn Bhd, C=MY | 6E523C 1D0654 4AB0 | RSA | 4096 | SHA512W ITHRSA | 2021-03-10 11:02:58 +08:00 | 2046-03-04 11:02:58 +08:00 | E6 72 1C 0D 75 19 9B 96 CFAC 6C 3B 91 1B A8A4 76 E2D5 97 | 0E FE 53 67 7F EF 63 1A 2A2F 8B 6FB1 B6 21 86 1B F5 73 52 EB85 70 26FE A9 B99E 7C 92 52 4D |

| CA | Subject DN | Issuer DN | Serial | Key Algorithm | Key Size (bits) | Digest Algorithm | Issuance Date | Expiration Date | Subject Key Identifier | Fingerprint SHA-256 |
|-----|--|--|--------------------------|---------------|-----------------|-------------------|----------------------------------|----------------------------------|--|---|
| 4.1 | CN=GPKI CA RSA, OU=MAMPU, O=Raffcomm Technologies Sdn Bhd, L=Putrajaya, ST=Wilayah Persekutuan, C=MY | CN=RAFFTECH Class 2 RSA Root CA, O=Raffcomm Technologies Sdn Bhd, C=MY | 60C8D4 DF7886 8B31 | RSA | 4096 | SHA256W ITHRSA | 2021-03-10 11:30:20 +08:00 | 2031-03-08 11:30:20 +08:00 | 73 1E ED41 5B 5411 09 18FD 66 38 B0 B7 CC0E 5D A4 90 B3 | 3E 47 3E E2 18 A1 A8 7D 33CD F9 4E 55 EA 0136 97 9D6E EB 4B9A 88 5F 51 FE 54B0 A1 010D 62 |