



Telekom Applied Business Sdn. Bhd.
2nd Floor, Kompleks TMIT,
Lingkaran Usahawan 1 Timur,
63300 Cyberjaya,
Selangor Darul Ehsan,
Malaysia

Report of Independent Accountant on Assessment of the Assertion by the management of Telekom Applied Business Sdn. Bhd. Certification Authority ("CA")

To: En. Thaib bin Mustafa
General Manager / Head of Telekom Applied Business Sdn Bhd.

We have been engaged to perform a reasonable assurance engagement on the accompanying assertion by the management of Telekom Applied Business Sdn. Bhd. Certification Authority ("TAB") for the period 1st April 2019 through 31st March 2020, for its Certification Authority ("CA") operations at Cyberjaya, Selangor, Malaysia, its CAs as enumerated in Appendix A.

Telekom Applied Business Sdn. Bhd. has:

- disclosed its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control practices in its Certificate Practice Statement and Certificate Policy;
- maintained effective controls to provide reasonable assurance that:
 - the CA provided its services in accordance with its Certification Practice Statement.
- maintained effective controls to provide reasonable assurance that:
 - logical and physical access to CA systems and data was restricted to authorized individuals; and
 - CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity.
- maintained effective controls to provide reasonable assurance that the integrity of keys and certificates it managed was established and protected throughout their life cycles;
- maintained effective controls to provide reasonable assurance that the following Root CA are used;
 - TM Applied Business Root Certificate



- maintained effective controls to provide reasonable assurance that the integrity of subscriber information was properly authenticated (for the registration activities performed Telekom Applied Business); and
- maintained effective controls to provide reasonable assurance that subordinate CA certificate requests were accurate, authenticated and approved,

in conformity with the CPA Canada Trust Services Principles and Criteria for Certification Authorities Version 2.1 (“CPA Canada WebTrust for Certification Authorities Criteria”).

Management’s Responsibility for the Management’s Assertion of Telekom Applied Business Certification Authority

Telekom Applied Business’s management is responsible for the preparation and presentation of the management’s assertion in accordance with the CPA Canada WebTrust for Certification Authorities Criteria.

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 Control 1, 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 Responsibility

It is our responsibility, to express a conclusion on the management’s assertion Telekom Applied Business based on our work performed and to report our conclusion solely to you, as a body, in accordance with our agreed terms of engagement, for management to submit to the related authority to continue displaying the WebTrust Seal on its website, and for no other purpose. We do not assume responsibility towards or accept liability to any other person for the contents of this report.

Telekom Applied Business makes use of external registration authorities for specific subscriber registration activities. Our assessment of Telekom Applied Business management assertion for the purpose of this WebTrust for CA certification examination did not extend to the controls of external registration authorities or the relevant systems and processes under the control of these external registration authorities.



The relative effectiveness and significance of specific controls at Telekom Applied Business 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 subscribers and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscribers and relying party locations.

We conducted our work in accordance with the International Standard on Assurance Engagements 3000 "Assurance Engagements Other Than Audits or Reviews of Historical Financial Information". This standard requires that we comply with ethical requirements and plan and perform the assurance engagement to obtain reasonable assurance over whether the management's assertion of Telekom Applied Business Certification Authority comply in all material respects with the CPA Canada WebTrust for Certification Authorities Criteria.

A reasonable assurance engagement involves performing procedures to obtain sufficient appropriate evidence over whether the management's assertion of Telekom Applied Business Certification Authority comply in all material respects with the CPA Canada WebTrust for Certification Authorities Criteria. The procedures selected depend on the auditor's judgment, including the assessment of the risks of material noncompliance of the management's assertion Telekom Applied Business Certification Authority with the CPA Canada WebTrust for Certification Authorities Criteria. Within the scope of our work we performed amongst others the following procedures: (1) obtaining an understanding of Telekom Applied Business's key and certificate life cycle management business and information privacy practices, and its controls over key and certificate integrity, over the authenticity and privacy of subscriber and relying party information, over the continuity of key and certificate life cycle management operations and over development, maintenance and operation of systems integrity; (2) selectively testing transactions executed in accordance with disclosed key and certificate life cycle management business and information privacy 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 conclusion.

Relative Effectiveness of Controls

The relative effectiveness and significance of specific controls at Telekom Applied Business 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 Limitation

We draw attention to the fact that the CPA Canada WebTrust for Certification Authorities Criteria includes certain inherent limitations that can influence the reliability of the information.

Because of inherent limitations in controls, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that (1) changes made to the system or controls, (2) changes in processing requirements, (3) changes required because of the passage of time, or (4) degree of compliance with the policies or procedures may alter the validity of such conclusions.

Emphasis of Matters

Without modifying our conclusion, we draw attention to the description of the non-compliances contained within the Report of Independent Accountant on Assessment of the Assertion by the management of Telekom Applied Business Sdn. Bhd. Certification Authority. This relates to:

- The annual testing of the CA's disaster recovery process for critical IT components of the CA system has not been performed; and
- Backup (for system and data) storage were not kept at an alternate location or site.

Throughout the audit period, there were no reported incidents that had resulted in disruption to the CA's business operations which requires Telekom Applied Business to invoke the IT disaster recovery systems, nor a need to recover data from the backup disks due to hazards within the data centres.

The remedial actions for the above non-compliances have been advised and, had been implemented and remediated by TAB as of 12th September 2020.

Opinion

In our opinion, throughout the period 1st April 2019 through 31st March 2020, Telekom Applied Business management's assertion, as referred to above, is fairly stated, in all material respects, in accordance with WebTrust Principles and Criteria for Certification Authorities Version 2.1.

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



Restriction on Use and Distribution

Our report is intended solely for the use of Telekom Applied Business to display the WebTrust Seal on its website after submitting the report to the related authority in connection with the CPA Canada WebTrust for Certification Authorities Criteria and may not be suitable for another purpose. This report is not intended to be, and should not be distributed to or used, for any other purpose.

Yours faithfully

PricewaterhouseCoopers PLT

PricewaterhouseCoopers PLT (LLP0014401-LCA & AF1146)

Kuala Lumpur, Malaysia

5th October 2020



Appendix A – Summary of work performed

Exceptions noted within scope of work based on CPA Canada Trust Services Principles and Criteria for Certification Authorities (“CA”)

Criterion No.	Section Name	Exceptions noted
1.1	Certification Practice Statement (CPS)	No
1.2	Certificate Policy	No
2.1	Certificate Policy Management	No
2.2	Certification Practice Statement Management	No
2.3	CP and CPS Consistency	No
3.1	Security Management	No
3.2	Asset Classification and Management	No
3.3	Personnel Security	No
3.4	Physical and Environmental Security	No
3.5	Operations Management	Yes
3.6	System Access Management	No
3.7	Systems Development and Maintenance	No
3.8	Business Continuity Management	Yes
3.9	Monitoring and Compliance	No
3.1	Audit Logging	No
4.1	CA Key Generation	No
4.2	CA Key Storage, Backup and Recovery	No



4.3	CA Public Key Distribution	No
4.4	CA Key Usage	No
4.5	CA Key Archival	No
4.6	CA Key Destruction	No
4.7	CA Key Compromise	No
4.8	CA Cryptographic Hardware Life Cycle Management	No
4.9	CA Key Escrow (if applicable)	No
4.1	CA Key Transportation (if applicable)	No
4.11	CA Key Migration (if applicable)	No
5.1	CA-Provided Subscriber Key Generation Services (if supported)	No
5.4	Requirements for Subscriber Key Management	No
6.1	Subscriber Registration	No
6.2	Certificate Renewal (if supported)	No
6.4	Certificate Issuance	No
6.5	Certificate Distribution	No
6.6	Certificate Revocation	No
6.7	Certificate Suspension (if supported)	No



6.8	Certificate Validation	No
7.1	Subordinate CA Certificate Life Cycle Management	No

APPENDIX B – TELEKOM APPLIED BUSINESS ROOT AND ISSUING CAs

Root CAs

Name	Certificate Thumbprint (sha256)
TM Applied Business Root Certificate	A9:C7:7A:F1:BC:DF:AA:37:39:44:2B:0B:27:34:C6:8E:AF:2E:98:33:F0:D7:66:FB:CA:A6:F2:AE:B4:2D:EC:02

Intermediates CAs

Name	Certificate Thumbprint (sha256)
TM Applied Business Certification Authority	5C:48:76:A2:88:43:6B:85:6D:C9:6C:A3:5B:76:CD:2D:B8:39:59:AF:86:5C:EF:56:6D:38:F5:9F:45:3C:57:05