Tel: +603 2616 2888
Fax: +603 2616 2829
www.bdo.my

Level 8
BDO @ Menara CenTARa
360 Jalan Tuanku Abdul Rahman
50100 Kuala Lumpur
Malaysia

INDEPENDENT ASSURANCE REPORT

To the management of Thai Digital ID Company Limited ("TDID"):

Scope

We have been engaged, in a reasonable assurance engagement, to report on TDID management's assertion that for its Certification Authority (CA) operations at Bangkok and Chonburi, Thailand, throughout the period 1 September 2022 to 31 August 2023 for its CA as below, TDID has:

Common Name	Certificate Serial No.	Subject Key Identifier	SHA-256 Fingerprint
Thai Digital ID CA G3	5152C650	477C0B4B1017E27D8091D5C140AA530B28B72F48	981D016EB85502B6DE8670598B2DD7A78525A391471F55542EEA2A27D812E4BF

- Disclosed its SSL certificate lifecycle management business practices in applicable versions of its Certification Practice Statements as enumerated in **Appendix A**, including its commitment to provided SSL certificate in conformity with CA/Browser Forum Requirements on the TDID website, and provided such services in accordance with its disclosed practices

- Maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and SSL certificates it manages is established and protected throughout their lifecycle; and
  - SSL subscriber information is properly authenticated (for the registration activities performed by TDID)

- 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 – SSL Baseline v2.7.

Certification authority's responsibilities

TDID'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 – SSL Baseline v2.7.

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.

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.

Practitioner'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 TDID's SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of SSL certificates;
(2) Selectively testing transactions executed in accordance with disclosed SSL certificate lifecycle management practices;
(3) Testing and evaluating the operating effectiveness of the controls;
(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.

The relative effectiveness and significance of specific controls at TDID 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

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.

Basis for Qualified Opinion

During our procedures, we noted the following that caused a qualification of our opinion:

No.	Observation	Relevant WebTrust Criteria
1	We noted that CRL reason codes have not been disclosed in the established Subscriber Agreement and/or CPS Section 4.9.1.1 as per the requirement of CABF Baseline Requirement documents. Additionally, users are required to only input their reason for revocation based on the revocation form available, however the specific reason codes as per CABF Baseline Requirement Section 7.2.2: CRL and CRL entry extensions were not fully implemented. This caused SSL Baseline v2.7, Principle 2; Criteria 2.18 and 5.3 to not be met.	**Principle 2 Criterion 2.18** The CA maintains controls to provide reasonable assurance that the version numbers and extensions of CRLs conform to the Baseline Requirements. **Principle 2 Criterion 5.3** The CA maintains controls to provide reasonable assurance that Subscriber Certificates are revoked within 24 hours for the specific events defined in the criterion.
2	We noted that CRL contained entries of suspended certificates (non-SSL) as a single CA is used to issue non-SSL and SSL certificates. This caused SSL Baseline v2.7, Principle 2; Criterion 5.8 to not be met.	**Principle 2 Criterion 5.8** The CA maintains controls to provide reasonable assurance that the CA does not remove revocation entries on a CRL or OCSP Response until after the Expiry Date of the revoked Certificate.

Qualified Opinion

In our opinion, except for the matters described in the basis for qualified opinion section above, throughout the period 1 September 2022 to 31 August 2023, TDID has, in all material respects:

- Disclosed its SSL certificate lifecycle management business practices in applicable versions of its Certification Practice Statements as enumerated in **Appendix A**, including its commitment to provided SSL certificate in conformity with CA/Browser Forum Requirements on the TDID website, and provided such services in accordance with its disclosed practices

- Maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and SSL certificates it manages is established and protected throughout their lifecycle; and
  - SSL subscriber information is properly authenticated (for the registration activities performed by TDID)

- 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 - SSL Baseline v2.7.

This report does not include any representation as to the quality of TDID's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities - SSL Baseline v2.7, nor the suitability of any of TDID's services for any customer's intended purpose.

BDO Consulting Sdn. Bhd.
Kuala Lumpur, Malaysia
27 August 2024

Appendix A – Certificate Policy and Certification Practice Statements in Scope

CP/CPS	Begin Effective Date	End Effective Date
Version 1.6	5 March 2021	6 April 2023
Version 1.7	7 April 2023	25 December 2023
Version 2.0	26 December 2023	11 January 2024
Version 2.1	12 January 2024	9 June 2024
Version 2.2	10 June 2024	-

Thai Digital ID Co., Ltd. 319ChamchuriSquareBuilding,25thFloor,Unit10-11Phayathai Rd,PathumwanBangkok10330
บริษัทไทยดิจิทัลไอดีจำกัด319อาคารจัตุรัสจามจุรีชั้น25 ห้อง10-11 ถนนพญาไทปทุมวัน กรุงเทพฯ10330
TEL.+66(0) 2029 0290 FAX.+66(0) 2029 0293 Website: http://www.thaidigitalid.com

19 July 2024

Assertion by Thai Digital ID Co. Ltd as to its Disclosure of its Business Practices and Controls over its Certification Authority Operations during the period from 1 September 2022 through 31 August 2023

Thai Digital ID Company Limited ("TDID") operates the Certification Authority (CA) services known as:

Common Name	Certificate Serial No.	Subject Key Identifier	SHA-256 Fingerprint
Thai Digital ID CA G3	5152C650	477C0B4B1017E27D8091D5C140AA530B28B72F48	981D016EB85502B6DE8670598B2DD7A78525A391471F55542EEA2A27D812E4BF

and provides SSL CA services.

The management of TDID is responsible for establishing and maintaining effective controls over its SSL CA operations, its SSL CA business practices disclosure on its website, SSL key lifecycle management controls, and SSL certificate lifecycle management controls. These controls contain monitoring mechanism, 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 TDID's CA operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

TDID management has assessed its disclosures of its certificate practices and controls over its SSL CA services. During our assessment, we noted the following observations which caused the relevant criteria to not be met:

No.	Observation	Relevant WebTrust Criteria
1	We noted that CRL reason codes have not been disclosed in the established Subscriber Agreement and/or CPS Section 4.9.1.1 as per the requirement of CABF Baseline Requirement documents. Additionally, users are required to only input their reason for revocation based on the revocation form available, however the specific reason code as per CABF Baseline Requirement Section 7.2.2: CRL and CRL entry extensions were not fully implemented.	**Principle 2 Criteria 2.18** The CA maintains controls to provide reasonable assurance that the version numbers and extensions of CRLs conform to the Baseline Requirements. **Principle 2 Criteria 5.3** The CA maintains controls to provide reasonable assurance that Subscriber Certificates are revoked within 24 hours for the specific events defined in the criterion.

	This caused SSL Baseline with Network Security 2.7, Principle 2; Criteria 2.18 and Criteria 5.3 to not be met	
2	We noted that CRL contained entries of suspended certificates (non-SSL) as a single CA is used to issue non-SSL and SSL certificates. This caused SSL Baseline with Network Security v2.7, Principle 2; Criterion 5.8 to not be met.	**Principle 2 Criterion 5.8** The CA maintains controls to provide reasonable assurance that the CA does not remove revocation entries on a CRL or OCSP Response until after the Expiry Date of the revoked Certificate.

Based on our assessment, in TDID management's opinion, except for the matters described in the preceding table, in providing its SSL CA services at Bangkok and Chonburi, Thailand, throughout the period 1 September 2022 to 31 August 2023, TDID has:

- disclosed its SSL certificate lifecycle management business practices in applicable versions of its Certification Practice Statement as enumerated in **Appendix A**, including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the TDID website and provide such services in accordance with its disclosed practices
- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and SSL certificates it manages is established and protected throughout their lifecycles; and
  - SSL subscriber information is properly authenticated (for the registration activities performed by TDID)
- 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 – SSL Baseline with Network Security v2.7.

Yours Faithfully,

d-Signature
d-sign
19/07/2567
08:28:39 +0700
วรวัฒน์ ภาอาภรณ์

Mr.Worawat Paarporn
Managing Director
Thai Digital ID Company Limited

Thai Digital ID Co., Ltd. 319ChamchuriSquareBuilding,25thFloor,Unit10-11Phayathai Rd,PathumwanBangkok10330
บริษัทไทยดิจิทัลไอดีจำกัด319อาคารจัตุรัสจามจุรีชั้น25 ห้อง10-11 ถนนพญาไทปทุมวัน กรุงเทพฯ10330
TEL.+66(0) 2029 0290 FAX.+66(0) 2029 0293 Website: http://www.thaidigitalid.com

Appendix A - Certificate Policy & Certification Practice Statements in Scope

CP/CPS	Begin Effective Date	End Effective Date
Version 1.6	5 March 2021	6 April 2023
Version 1.7	7 April 2023	25 December 2023
Version 2.0	26 December 2023	11 January 2024
Version 2.1	12 January 2024	9 June 2024
Version 2.2	10 June 2024	-