



日盛聯合會計師事務所
SUN RISE CPAS' FIRM
DFK INTERNATIONAL



19F.-5, No.171, Songde Rd., Sinyi District,
Taipei City 110, TW.
Tel : +886 2 2346 6168
Fax : +886 2 2346 6068

INDEPENDENT ASSURANCE REPORT

To the management of Internet Thailand Public Company Limited. (INET):

We have been engaged, in a reasonable assurance engagement, to report on INET management's assertion that for its Certification Authority (CA) operations at locations as enumerated at Bangkok, Thailand, throughout the period 18 December 2024 to 17 December 2025 for its INET CA - G1 (INET CA) as enumerated in Appendix A, INET has:

- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

in accordance with the [WebTrust Principles and Criteria for Certification Authorities – Network Security, v1.7.](#)

Certification authority's responsibilities

INET's management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance the [WebTrust Principles and Criteria for Certification Authorities – Network Security, v1.7.](#)

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 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.

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 INET's network and certificate system security to meet the requirements set forth by the CA/Browser Forum;
- (2) testing and evaluating the operating effectiveness of the controls; and
- (3) 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 INET 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 matters which caused a qualification of our opinion:

Observations	Relevant WebTrust Criteria
<p>We noted that the VPN service responsible for network boundary access control did not enable its Multi-Factor authentication mechanism for specific accounts.</p> <p>This caused WebTrust Principles and Criteria for Certification Authorities – Network Security – Version 1.7, Criterion 2.7 to not be met.</p> <p>We have received evidence for remediations</p>	<p>2.7 The CA maintains controls to provide reasonable assurance that Trusted Role using a username and password to authenticate shall configure accounts to include but not be limited to:</p> <ul style="list-style-type: none"> - For authentications which cross a zone boundary into a Secure Zone or High-Security Zone: <ul style="list-style-type: none"> • Require Multi-Factor Authentication;



日盛聯合會計師事務所
SUN RISE CPAS' FIRM
DFK INTERNATIONAL



19F.-5, No.171, Songde Rd., Sinyi District,
Taipei City 110, TW.
Tel : +886 2 2346 6168
Fax : +886 2 2346 6068

<p>on the deviation from compliance prior to the issuance of this report.</p>	
<p>We noted that the 2025 Q2 Vulnerability Scan was not conducted within three months after Vulnerability Scan conducted in previous quarter.</p> <p>This caused WebTrust Principles and Criteria for Certification Authorities – Network Security – Version 1.7, Criterion 4.3 to not be met.</p>	<p>4.3 The CA maintains controls to provide reasonable assurance that a Vulnerability Scan is performed on public and private IP addresses identified by the CA or Delegated Third Party as the CA's or Delegated Third Party's Certificate Systems based on the following:</p> <ul style="list-style-type: none"> • At least every three (3) months.

Qualified opinion

In our opinion, except for the matters described in the basis for qualified section above, throughout the period 18 December 2024 to 17 December 2025, INET 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 – Network Security, v1.7](#).

This report does not include any representation as to the quality of INET's services beyond those covered by the [WebTrust Principles and Criteria for Certification Authorities – Network Security, v1.7](#), nor the suitability of any of INET's services for any customer's intended purpose.

Use of the WebTrust seal

INET's use of the WebTrust Principles and Criteria for Certification Authorities – Network Security 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.



日盛聯合會計師事務所
SUN RISE CPAS' FIRM
DFK INTERNATIONAL

March 16, 2026

DFK INTERNATIONAL



日盛聯合會計師事務所
SUN RISE CPAS' FIRM
DFK INTERNATIONAL



19F.-5, No.171, Songde Rd., Sinyi District,
Taipei City 110, TW.
Tel : +886 2 2346 6168
Fax : +886 2 2346 6068

Appendix A – CAs within the Scope of Audit

INET CA – G1	
Subject	Issuer
CN = INET CA - G1 O = Internet Thailand Public Company Limited C = TH	CN = Thailand National Root Certification Authority - G1 OU = Thailand National Root Certification Authority O = Electronic Transactions Development Agency (Public Organization) C = TH
Certificate Related Information	Key Related Information
Serial Number: 485F534C000000005152C73D Signature Algorithm: sha512RSA Not Before: Nov 26 07:06:53 2018 GMT Not After : Nov 25 17:00:00 2034 GMT Thumbprint Algorithm: sha1 Thumbprint:C2F88A712E5775DE623B9A51391F4B52DE20BF89 Thumbprint Algorithm: sha256 Thumbprint:DABF2E406C3DA1FE15166596E9029FADB1C3DFF59670D8AC5BFB6345198BC1AA	Subject Public Key: RSA(4096 bits) Subject Key Identifiers: B7D2C425A677250896569C9FAF18CC2ACF2B78CF Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)



MANAGEMENT’S ASSERTION

Internet Thailand Public Company Limited. (“INET”) operates the Certification Authority (CA) services known as INET Certification Authority (INET CA) listed in Appendix A and provides CA services.

The management of INET CA is responsible for establishing and maintaining effective controls over its CA operations, including its network and certificate security system 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 INET CA’s Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

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

Observations	Relevant WebTrust Criteria
<p>We noted that the VPN service responsible for network boundary access control did not enable its Multi-Factor authentication mechanism for specific accounts.</p> <p>This caused WebTrust Principles and Criteria for Certification Authorities –</p>	<p>2.7 The CA maintains controls to provide reasonable assurance that Trusted Role using a username and password to authenticate shall configure accounts to include but not be limited to:</p>



<p>Network Security – Version 1.7, Criterion 2.7 to not be met.</p>	<ul style="list-style-type: none"> - For authentications which cross a zone boundary into a Secure Zone or High-Security Zone: <ul style="list-style-type: none"> • Require Multi-Factor Authentication;
<p>We noted that the 2025 Q2 Vulnerability Scan was not conducted within three months after Vulnerability Scan conducted in previous quarter.</p> <p>This caused WebTrust Principles and Criteria for Certification Authorities – Network Security – Version 1.7, Criterion 4.3 to not be met.</p>	<p>4.3 The CA maintains controls to provide reasonable assurance that a Vulnerability Scan is performed on public and private IP addresses identified by the CA or Delegated Third Party as the CA’s or Delegated Third Party’s Certificate Systems based on the following:</p> <ul style="list-style-type: none"> • At least every three (3) months.

INET CA management has assessed its controls over its CA services. Based on that assessment, except for the matters described in the preceding table, in providing its CA services at Bangkok, Thailand, throughout the period 18 December 2024 to 17 December 2025, INET has:

- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

in accordance with [WebTrust Principles and Criteria for Certification Authorities – Network Security – Version 1.7](#).



Appendix A – CAs within the Scope of Audit

INET CA – G1	
Subject	Issuer
CN = INET CA - G1 O = Internet Thailand Public Company Limited C = TH	CN = Thailand National Root Certification Authority - G1 OU = Thailand National Root Certification Authority O = Electronic Transactions Development Agency (Public Organization) C = TH
Certificate Related Information	Key Related Information
Serial Number: 485F534C000000005152C73D Signature Algorithm: sha512RSA Not Before: Nov 26 07:06:53 2018 GMT Not After : Nov 25 17:00:00 2034 GMT Thumbprint Algorithm: sha1 Thumbprint:C2F88A712E5775DE623B9A51391F4B52DE20BF89 Thumbprint Algorithm: sha256 Thumbprint:DABF2E406C3DA1FE15166596E9029FADB1C3DFF59670D8AC5BFB6345198BC1AA	Subject Public Key: RSA(4096 bits) Subject Key Identifiers: B7D2C425A677250896569C9FAF18CC2ACF2B78CF Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)