Independent Assurance Report

To the management of the Ministry of Digital Affairs：

Scope

We have been engaged, in a reasonable assurance engagement, to report on Ministry of Digital Affairs (MODA) management's assertion that for its Certification Authority (CA) operations at Taipei and Taichung, Taiwan, throughout the period October 1, 2023 to September 30, 2024 for its CA in Appendix A for SSL Baseline with Network Security Requirements, MODA has:

- Disclosed its SSL certificate lifecycle management business practices in its:
  - GTLSCA Certification Practice Statement V1.0.4
  - Certificate Policy for the Chunghwa Telecom ecommerce Public Key Certificate Policy V2.1 （Maintained and manage By Chunghwa Telecom）

  including its commitment to provide SSL certificates in conformity with the CA/Browser Forum requirements on the GTLSCA websites, 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 lifecycles; and
  - SSL certificate subscriber information is properly authenticated for the registration activities performed by GTLSCA.

- 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
- 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 – SSL Baseline with Network Security V2.7.

Certification authority's responsibilities

MODA'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 with Network Security 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 Control 1, Quality Control for Firms that perform Audits and Reviews of Historical Financial Information, other Assurance and Related Service 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.

KPMG auditor team qualifications are listed in Appendix B.

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 GTLSCA's SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of SSL certificates, and obtaining an understanding of GTLSCA's network and certificate system security to meet the requirements set forth by the CA/Browser Forum;

(2) selectively testing transactions executed in accordance with disclosed SSL certificate lifecycle management 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.

GTLSCA' s management has disclosed to KPMG the incidents as detailed in Appendix C that have been posted in Bugzilla website that can be accessed publicly, from October 1, 2023 to September 30, 2024.

Relative effectiveness of controls

The relative effectiveness and significance of specific controls at GTLSCA 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, GTLSCA's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorized 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.

Basis for qualified opinion

During our examination, we noted the following which caused a qualification of our opinion:

Observation	Relevant WebTrust Criteria
During the period, upon the discovery of the revoke certification, any of the following did not occur within 5 days： 1. Since the twice CAB incident notification related to the certificate revocation, GTLSCA has taken over a month to complete for 2 cases. For each process, GTLSCA only keep one documented record and lacks a timelines log. 2. During the audit period, there were two similar incidents in total that did not meet the requirement of being revoked within 5 days, and there is no clear evidence to support any corrective and preventive remedy for such incident until July 23, 2024.	WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – V2.7 5.3 And, Subscriber Certificates are revoked within 5 days if any of the following events occurs: 8.The CA determines that any of the information appearing in the Certificate is inaccurate;

Qualified Opinion

In our opinion, except for the matters described in the Basis for qualified opinion section of our report, throughout the period October 1, 2023 to September 30, 2024, MODA 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 – SSL Baseline with Network Security V2.7.

This report does not include any representation as to the quality of GTLSCA's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security V2.7, nor the suitability of any of GTLSCA's services for any customer's intended purpose.

Use of the WebTrust seal

GTLSCA's use of the WebTrust for Certification Authorities – SSL Baseline with 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.

Chen, Pei Chi, KPMG

KPMG

Certified Public Accountants

Taipei, Taiwan, ROC

November 8, 2024

Appendix A

<table>
<tr><td rowspan="6">ePKI Root Certification Authority - G2[1]</td><td colspan="2">Issuer Root CA Certificate</td></tr>
<tr><td>Subject</td><td>Issuer</td></tr>
<tr><td>CN = ePKI Root Certification Authority - G2
O= Chunghwa Telecom Co., Ltd.
C=TW</td><td>CN = ePKI Root Certification Authority
O = Chunghwa Telecom Co., Ltd.
C=TW</td></tr>
<tr><td>Certificate Related Information</td><td>Key Related Information</td></tr>
<tr><td>Serial Number: 3beee0918e8886ad460fe8ae910c9cba
Signature Algorithm: sha256RSA
Not Before: 2015-11-17 04:51:35 p.m.(UTC+8:00)
Not After: 2034-12-20 10:31:27 a.m.(UTC+8:00)
Thumbprint Algorithm: sha256
Thumbprint: 64717250af8b028dd8e5c0bae4c9142c8b103532612bc487085fd3c319f9c067</td><td>Subject Public Key: RSA(4096 bits)
Authority Key Identifiers: 1e0cf7b667f2e192260945c055392e773f424aa2
Subject Key Identifiers: 725bbaaa7238ee259024b59422fa0988ca8b0afb
Basic Constraint: Subject Type=CA
Path Length Constraint=None
Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)</td></tr>
<tr><td>Additional Information</td><td>Remark</td></tr>
<tr><td>CRL Distribution Point: http://eca.hinet.net/repository/CRL_SHA2/CA.crl
[1]Certificate Policy:
Policy Identifier=1.3.6.1.4.1.23459.100.0.1
[2]Certificate Policy:
Policy Identifier=1.3.6.1.4.1.23459.100.0.2
[3]Certificate Policy:
Policy Identifier=1.3.6.1.4.1.23459.100.0.3</td><td>■ CA certificate Generation of ePKI Root Certification Authority - G2 signed by ePKI Root Certification Authority</td></tr>
</table>

[1] ePKI Root CA is audited by Chunghwa itself and not included in this audit.

	[4]Certificate Policy: Policy Identifier=1.3.6.1.4.1.23459.100.0.4 [5]Certificate Policy: Policy Identifier=1.3.6.1.4.1.23459.100.0.9 [6]Certificate Policy: Policy Identifier=1.3.6.1.4.1.23459.100.0.0 [7]Certificate Policy: Policy Identifier=2.16.886.1.100.0.1 [8]Certificate Policy: Policy Identifier=2.16.886.1.100.0.2 [9]Certificate Policy: Policy Identifier=2.16.886.1.100.0.3 [10]Certificate Policy: Policy Identifier=2.16.886.1.100.0.4 [11]Certificate Policy: Policy Identifier=2.16.886.1.100.0.0 [12]Certificate Policy: Policy Identifier=2.23.140.1.2.1 [13]Certificate Policy: Policy Identifier=2.23.140.1.2.2 [14]Certificate Policy: Policy Identifier=2.23.140.1.2.3 [15]Certificate Policy: Policy Identifier=2.23.140.1.1 [15,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://eca.hinet.net/repository	

GTLSCA – G1	Subordinate CA Certificate	
	Subject	Issuer
	CN = Government TLS Certification Authority- G1 O=Executive Yuan C=TW	CN = ePKI Root Certification Authority - G2 O = Chunghwa Telecom Co., Ltd. C=TW
	Certificate Related Information	Key Related Information
	Serial Number: 00996d5fe9ade16cdc8ecdbfedb14a3295 Signature Algorithm: sha256RSA Not Before: 2019-07-19 14:46:45 p.m.(UTC+8:00) Not After: 2031-08-19 14:46:45 p.m.(UTC+8:00) Thumbprint Algorithm: sha1 Thumbprint: b2d151a768d30c3b99d86b8b25815608c28ab2cb Thumbprint Algorithm: sha256 Thumbprint: 9d1cda1b9ef395afce7de0fe74de6d9ff5e0d2a43789116c00c6ba5bf44b9823	Subject Public Key: RSA(4096 bits) Authority Key Identifiers: 725bbaaa7238ee259024b59422fa0988ca8b0afb Subject Key Identifiers: d6eb2d9d61fe2bbb70882eb807b159b0f483226a Basic Constraint: Subject Type=CA Path Length Constraint=0 Key Usage: Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)
	Additional Information	Remark
	CRL Distribution Point: http://eca.hinet.net/repository/CRL2/CA.crl [1].Certificate Policy: 1.3.6.1.4.1.23459.100.0.3 [2].Certificate Policy: 2.23.140.1.2.2	■ CA certificate of 1st Generation of GTLSCA signed by ePKI Root Certification Authority - G2

Appendix B

KPMG Audit Team has a qualified firm and practitioners, provide assurance and attest reports as part of the Firm's regular business activities and the standards set out in the WebTrust Agreement. A Qualified Firm follows recognized professional auditing standards as published by the International Federation of Accountants (IFAC), the American Institute of Certified Public Accountants (AICPA) or the Chartered Professional Accountants of Canada (CPA Canada). In addition, practitioners/staff have the necessary technical training, competency and experience to conduct a WebTrust for Certification Authorities engagement in accordance with professional auditing standards.

Team Member	Title	Certifications	Years of Experience	Years of Experience with PKI
Team Leader	Partner	CISA,IRCA Registered ISO 27001 LA	More than 21 years	More than 12 years
Member A	Manager	CISA, ISO 27001 LA	More than 16 years	More than 13 years
Member B	Assistant Manager	ISO 27001 LA	More than 7 years	More than 7 years
Member C	Senior Consultant	ISO 27001 LA	More than 6 years	More than 7 years
Member D	Senior Consultant	CEH,CCNA, ISO 27001 LA	More than 7 years	More than 5 years

Appendix C

No	Time	Subject	Publicly Link
1	03.22.2024	Chunghwa Telecom: Wrong Extended Key Usage setting by GTLSCA	BugZilla Ticket Link
2	04.19.2024	Chunghwa Telecom: Delayed Revocation Due to GTLSCA EKU Misissuance	BugZilla Ticket Link
3	05.23.2024	Chunghwa Telecom: Controversial Values within Extension (2.5.29.9, subjectDirectoryAttributes)	BugZilla Ticket Link
4	06.17.2024	Chunghwa Telecom: Delayed Revocation with Controversial Extension (2.5.29.9, SubjectDirectoryAttributes)	BugZilla Ticket Link
5	09.03.2024	Chunghwa Telecom: TLS Certificates Contains two LocalityName Values in SubjectDN by GTLSCA	BugZilla Ticket Link

數位發展部
Ministry of Digital Affairs

Assertion of Management as to
its Disclosure of its Business Practices and it Controls Over
its Certification Authority Operations
during the period from October 1, 2023 through September 30, 2024

November 8, 2024

The Ministry of Digital Affairs (MODA) operates the Certification Authority (CA) services known as Government TLS Certification Authority (GTLSCA) in Appendix A and provides SSL CA services.

The management of GTLSCA is responsible for establishing and maintaining effective controls over its SSL CA operations, including its network and certificate security system controls,its SSL CA business practices disclosure on its website ,SSL key lifecycle management controls, and SSL 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 of controls. Accordingly, even effective controls can only provide reasonable assurance with respect to GTLSCA's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

MODA management has assessed its disclosures of its certificate practices and controls over its SSL CA services. Based on that assessment, in providing its SSL Certification Authority services at Taipei and Taichung, Taiwan, throughout the period October 1, 2023 to September 30, 2024, GTLSCA has:

■ disclosed its SSL certificate lifecycle management business practices in its:

— GTLSCA Certification Practice Statement V1.0.4

— Certificate Policy for the Chunghwa Telecom ecommerce Public Key Certificate Policy V2.1 （Maintained and manage By Chunghwa Telecom）

including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the GTLSCA 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 lifecycles; and
  - SSL certificate subscriber information is properly authenticated for the registration activities performed by GTLSCA

- 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

- 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

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

Observation	Relevant WebTrust Criteria
During the period, upon the discovery of the revoke certification, any of the following did not occur within 5 days： 1. Since the twice CAB incident notification related to the certificate revocation, GTLSCA has taken over a month to complete for 2 cases. For each process, GTLSCA only keep one documented record and lacks a timelines log. 2. During the audit period, there were two similar incidents in total that did not meet the requirement of being revoked within 5 days, and there is no clear evidence to support any corrective and preventive remedy for such incident until July 23, 2024.	WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – V 2.7 5.3 And, Subscriber Certificates are revoked within 5 days if any of the following events occurs: 8.The CA determines that any of the information appearing in the Certificate is inaccurate;

in accordance with the WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security v2.7.

Ministry of Digital Affairs

November 8, 2024

Appendix A

<table>
<tr><td rowspan="6">ePKI Root Certification Authority - G2</td><td colspan="2">Issuer Root CA Certificate</td></tr>
<tr><td>Subject</td><td>Issuer</td></tr>
<tr><td>CN = ePKI Root Certification Authority - G2
O= Chunghwa Telecom Co., Ltd.
C=TW</td><td>CN = ePKI Root Certification Authority
O = Chunghwa Telecom Co., Ltd.
C=TW</td></tr>
<tr><td>Certificate Related Information</td><td>Key Related Information</td></tr>
<tr><td>Serial Number:
3beee0918e8886ad460fe8ae910c9cba
Signature Algorithm: sha256RSA
Not Before: 2015-11-17 04:51:35 p.m.(UTC+8:00)
Not After: 2034-12-20 10:31:27 a.m.(UTC+8:00)
Thumbprint Algorithm: sha256
Thumbprint:
64717250af8b028dd8e5c0bae4c9142c8b103532612bc487085fd3c319f9c067</td><td>Subject Public Key: RSA(4096 bits)
Authority Key Identifiers:
1e0cf7b667f2e192260945c055392e773f424aa2
Subject Key Identifiers:
725bbaaa7238ee259024b59422fa0988ca8b0afb
Basic Constraint: Subject Type=CA
Path Length Constraint=None
Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)</td></tr>
<tr><td>Additional Information</td><td>Remark</td></tr>
<tr><td>CRL Distribution Point:
http://eca.hinet.net/repository/CRL_SHA2/CA.crl
[1]Certificate Policy:
Policy Identifier=1.3.6.1.4.1.23459.100.0.1
[2]Certificate Policy:
Policy Identifier=1.3.6.1.4.1.23459.100.0.2
[3]Certificate Policy:
Policy Identifier=1.3.6.1.4.1.23459.100.0.3
[4]Certificate Policy:
Policy Identifier=1.3.6.1.4.1.23459.100.0.4
[5]Certificate Policy:
Policy</td><td>■ CA certificate Generation of ePKI Root Certification Authority - G2 signed by ePKI Root Certification Authority</td></tr>
</table>

	Identifier=1.3.6.1.4.1.23459.100.0.9 [6]Certificate Policy: Policy Identifier=1.3.6.1.4.1.23459.100.0.0 [7]Certificate Policy: Policy Identifier=2.16.886.1.100.0.1 [8]Certificate Policy: Policy Identifier=2.16.886.1.100.0.2 [9]Certificate Policy: Policy Identifier=2.16.886.1.100.0.3 [10]Certificate Policy: Policy Identifier=2.16.886.1.100.0.4 [11]Certificate Policy: Policy Identifier=2.16.886.1.100.0.0 [12]Certificate Policy: Policy Identifier=2.23.140.1.2.1 [13]Certificate Policy: Policy Identifier=2.23.140.1.2.2 [14]Certificate Policy: Policy Identifier=2.23.140.1.2.3 [15]Certificate Policy: Policy Identifier=2.23.140.1.1 [15,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://eca.hinet.net/repository	

<table>
<tr><td rowspan="6">GTLSCA – G1</td><td colspan="2">Subordinate CA Certificate</td></tr>
<tr><td>Subject</td><td>Issuer</td></tr>
<tr><td>CN = Government TLS Certification Authority- G1
O=Executive Yuan
C=TW</td><td>CN = ePKI Root Certification Authority - G2
O = Chunghwa Telecom Co., Ltd.
C=TW</td></tr>
<tr><td>Certificate Related Information</td><td>Key Related Information</td></tr>
<tr><td>Serial Number: 00996d5fe9ade16cdc8ecdbfedb14a3295
Signature Algorithm: sha256RSA
Not Before: 2019-07-19 14:46:45 a.m.(UTC+8:00)
Not After: 2031-08-19 04:46:45 p.m.(UTC+8:00)
Thumbprint Algorithm: sha1
Thumbprint: b2d151a768d30c3b99d86b8b25815608c28ab2cb
Thumbprint Algorithm: sha256
Thumbprint: 9d1cda1b9ef395afce7de0fe74de6d9ff5e0d2a43789116c00c6ba5bf44b9823</td><td>Subject Public Key: RSA(4096 bits)
Authority Key Identifiers: 725bbaaa7238ee259024b59422fa0988ca8b0afb
Subject Key Identifiers: d6eb2d9d61fe2bbb70882eb807b159b0f483226a
Basic Constraint: Subject Type=CA
Path Length Constraint=0
Key Usage: Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)</td></tr>
<tr><td>Additional Information</td><td>Remark</td></tr>
<tr><td>CRL Distribution Point: http://eca.hinet.net/repository/CRL2/CA.crl
[1].Certificate Policy: 1.3.6.1.4.1.23459.100.0.3
[2].Certificate Policy: 2.23.140.1.2.2</td><td>■ CA certificate of 1st Generation of GTLSCA signed by ePKI Root Certification Authority - G2</td></tr>
</table>