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, Taiwan, R.O.C.
Tel : +886 2 2346 6168
Fax : +886 2 2346 6068

INDEPENDENT ASSURANCE REPORT

To the management of Chunghwa Telecom (CHT):

We have been engaged, in a reasonable assurance engagement, to report on CHT management's assertion that for its Certification Authority (CA) operations at Taipei and Taichung, Taiwan, throughout the period 1 June 2019 to 31 May 2020 for its CAs as enumerated in Appendix A, CHT has:

- Disclosed its EV Certificate life cycle management practices and procedures, including its commitment to provide EV Certificates in conformity with the CA/Browser Forum Guidelines, and provided such services in accordance with disclosed practices in its certification practice statements and certificate policies listed in Appendix B.

- maintained effective controls to provide reasonable assurance that:
    - the integrity of keys and EV SSL certificates it manages is established and protected throughout their lifecycles; and
    - EV SSL certificate subscriber information is properly authenticated

in accordance with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL V1.6.8.

CHT does not escrow its CA keys and does not provide certificate suspension services. Accordingly, our procedures does not extend to controls that would address those criteria.

Certification authority's responsibilities

CHT'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 – Extended Validation SSL V1.6.8.

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,

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

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 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 CHT's EV SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of EV SSL certificates;
(2) selectively testing transactions executed in accordance with disclosed EV SSL certificate lifecycle management business 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.

Relative effectiveness of controls

The relative effectiveness and significance of specific controls at CHT 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, CHT's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or

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, Taiwan, R.O.C.
Tel : +886 2 2346 6168
Fax : +886 2 2346 6068

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.

Opinion

In our opinion, throughout the period 1 June 2019 to 31 May 2020, CHT 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 – Extended Validation SSL V1.6.8.

This report does not include any representation as to the quality of CHT's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL V1.6.8, nor the suitability of any of CHT's services for any customer's intended purpose.

Use of the WebTrust seal

CHT's use of the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL 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

August 24, 2020

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, Taiwan, R.O.C.
Tel : +886 2 2346 6168
Fax : +886 2 2346 6068

Appendix A-List of CAs in Scope

Root CAs										
Common Name	**Subject**	**Issuer**	**Serial**	**Key Algorithm**	**Key Size**	**Sig. Algorithm**	**Not Before**	**Not After**	**SKI**	**SHA256 Fingerprint**
HiPKI Root CA - G1	C=TW, O=Chunghwa Telecom Co., Ltd., CN=HiPKI Root CA - G1	C=TW, O=Chunghwa Telecom Co., Ltd., CN=HiPKI Root CA - G1	2dddacce629794a143e8b0cd766a5e60	rsaEncryption	4096 bits	sha256WithRSAEncryption	Feb 22 09:46:04 2019 GMT	Dec 31 15:59:59 2037 GMT	f27717fa5ea8fef63d71d568bac9460c38d8afb0	f015ce3cc239bfef064be9f1d2c417e1a0264a0a94be1f0c8d121864eb6949cc

EV SSL Issuing CAs										
Common Name	**Subject**	**Issuer**	**Serial**	**Key Algorithm**	**Key Size**	**Sig. Algorithm**	**Not Before**	**Not After**	**SKI**	**SHA256 Fingerprint**
HiPKI EV TLS CA - G1	C=TW, O=Chunghwa Telecom Co., Ltd., CN=HiPKI EV TLS CA - G1	C=TW, O=Chunghwa Telecom Co., Ltd., CN=HiPKI Root CA - G1	3c43cdcddcf23b004f0ea073fc3ea389	rsaEncryption	4096 bits	sha256WithRSAEncryption	Feb 22 09:56:03 2019 GMT	Dec 31 15:59:59 2037 GMT	a90dea63aee38c0340e7ffdc3328e5238ecb109b	2a8e6a86e74d10edb2026c81693d64957a0f081c1631912ac95efdfcb5625657

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, Taiwan, R.O.C.
Tel : +886 2 2346 6168
Fax : +886 2 2346 6068

Appendix B- Certificate Policy and Certification Practice Statement Versions in Scope

Document Name	Version	Effective Date
HiPKI CP	V1.05	March 2, 2020
HiPKI CP	V1.0	February 22, 2019
HiPKI RCA CPS	V1.05	March 2, 2020
HiPKI RCA CPS	V1.0	February 22, 2019
EV TLS CA CPS	V1.05	March 2, 2020
EV TLS CA CPS	V1.0	February 22, 2019

中華電信

MANAGEMENT'S ASSERTION OF CHUNGHWA TELECOM

Chunghwa Telecom (CHT) operates the Certification Authority (CA) services known as CAs in the Appendix A, and provides extended validation SSL (EV SSL) CA services.

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

CHT management has assessed its disclosures of its EV SSL practices and controls over its EV SSL CA services. Based on that assessment, in CHT management's opinion, in providing its EV SSL CA services at Taipei and Taichung, Taiwan, throughout the period1 June 2019 to 31 May 2020, CHT has:

- disclosed its EV SSL certificate lifecycle management business practices in the applicable versions of its CHT Certification Practice Statement ("CPS") and CHT Certificate Policy ("CP") as enumerated in Appendix B.

- maintained effective controls to provide reasonable assurance that:

- the integrity of keys and EV SSL certificates it manages is established and protected throughout their lifecycles; and
- EV SSL certificate subscriber information is properly authenticated;

in accordance with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL V1.6.8.

Signature: PETER LIN

Title: Vice President

August 24, 2020

中華電信

Appendix A-List of CAs in Scope

Root CAs										
Common Name	**Subject**	**Issuer**	**Serial**	**Key Algorithm**	**Key Size**	**Sig. Algorithm**	**Not Before**	**Not After**	**SKI**	**SHA256 Fingerprint**
HiPKI Root CA - G1	C=TW, O=Chunghwa Telecom Co., Ltd., CN=HiPKI Root CA - G1	C=TW, O=Chunghwa Telecom Co., Ltd., CN=HiPKI Root CA - G1	2dddacce629794a143e8b0cd766a5e60	rsaEncryption	4096 bits	sha256WithRSAEncryption	Feb 22 09:46:04 2019 GMT	Dec 31 15:59:59 2037 GMT	f27717fa5ea8fef63d71d568bac9460c38d8afb0	f015ce3cc239bfef064be9f1d2c417e1a0264a0a94be1f0c8d121864eb6949cc

EV SSL Issuing CAs										
Common Name	**Subject**	**Issuer**	**Serial**	**Key Algorithm**	**Key Size**	**Sig. Algorithm**	**Not Before**	**Not After**	**SKI**	**SHA256 Fingerprint**
HiPKI EV TLS CA - G1	C=TW, O=Chunghwa Telecom Co., Ltd., CN=HiPKI EV TLS CA - G1	C=TW, O=Chunghwa Telecom Co., Ltd., CN=HiPKI Root CA - G1	3c43cdcddcf23b004f0ea073fc3ea389	rsaEncryption	4096 bits	sha256WithRSAEncryption	Feb 22 09:56:03 2019 GMT	Dec 31 15:59:59 2037 GMT	a90dea63aee38c0340e7ffdc3328e5238ecb109b	2a8e6a86e74d10edb2026c81693d64957a0f081c1631912ac95efdfcb5625657

Appendix B- Certificate Policy and Certification Practice Statement Versions in Scope

Document Name	Version	Effective Date
HiPKI CP	V1.05	March 2, 2020
HiPKI CP	V1.0	February 22, 2019
HiPKI RCA CPS	V1.05	March 2, 2020
HiPKI RCA CPS	V1.0	February 22, 2019
EV TLS CA CPS	V1.05	March 2, 2020
EV TLS CA CPS	V1.0	February 22, 2019