



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 Co., Ltd. (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 locations as enumerated in Appendix B, throughout the period 26 October 2025 to 31 May 2026 for its CAs as enumerated in Appendix A, CHT has:

- disclosed its TLS certificate life cycle management business practices in in the applicable versions of its CHT Certification Practice Statement ("CPS") and CHT Certificate Policy ("CP") as enumerated in Appendix B including its commitment to provide TLS certificates in conformity with the CA/Browser Forum Requirements on the CHT website, and provided such services in accordance with its disclosed practices
- maintained effective controls to provide reasonable assurance that:
 - the integrity of keys and TLS certificates it manages is established and protected throughout their lifecycles; and
 - TLS certificate subscriber information is properly authenticated
- 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 – TLS Baseline v2.9.

The CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates require the CA to operate controls to adhere to the Network and Certificate System Security Requirements. The WebTrust



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

Principles and Criteria for Certification Authorities – Network Security address this requirement and are reported on in a separate report.

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 – TLS Baseline v2.9.

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.

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 TLS certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of TLS certificates;
- (2) selectively testing transactions executed in accordance with disclosed TLS



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

- 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 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 26 October 2025 to 31 May 2026, 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 – TLS Baseline v2.9.

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 – TLS Baseline v2.9, nor the suitability of any of CHT's services for any customer's intended purpose.



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

Other Matter

While the CHT's assertion notes all issues disclosed on Bugzilla through the audit period of this report, we have noted no instances relevant to the CAs enumerated in Appendix A or applicable to the WebTrust Principles and Criteria for Certification Authorities – TLS Baseline v2.9.

Use of the WebTrust seal

CHT's use of the WebTrust for Certification Authorities – TLS Baseline 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 10, 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, Taiwan, R.O.C.
Tel : +886 2 2346 6168
Fax : +886 2 2346 6068

Appendix A-List of CAs in Scope(TLS Baseline)

Root CAs										
Common Name	Subject	Issuer	Serial	Key Algorithm	Key Size	Sig. Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
CHT TrustRoot CA - G1	CN=CHT TrustRoot CA - G1, O=Chunghwa Telecom Co., Ltd., C=TW	CN=CHT TrustRoot CA - G1, O=Chunghwa Telecom Co., Ltd., C=TW	00e9bd907dc13595ccb590fa5d39e572a	rsaEncryption	4096 bits	sha256WithRSAEncryption	Aug 25 06:42:38 2025 GMT	Aug 25 15:59:59 2040 GMT	a48b5449e90eb52a03ac16256ca6d101c9bd61ef	AC0B9F8E3F88C9B A1FACA0B360B6EC 3DE1E2C7BE0EB50 8C063649ABA0206 1D39

OV TLS Issuing CA										
Common Name	Subject	Issuer	Serial	Key Algorithm	Key Size	Sig. Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
CHT Trust TLS CA - G1	CN = CHT Trust TLS CA - G1 O = Chunghwa Telecom Co., Ltd. C = TW	CN = CHT TrustRoot CA - G1 O = Chunghwa Telecom Co., Ltd. C = TW	709f59d2919894b8cd84205dc7015184	rsaEncryption	4096 bits	sha256WithRSAEncryption	Mar 12, 2026 02:53:09 GM	Mar 10, 2029 15:59:59 GMT	c78d5d8daae8214edb2f6372f2b57820f02bf861	14E9217404AC6F44 43A622F3061CF5FD F10D2C6F9448EB4 A1A25026FED2473 11



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-1 Certificates of CAs Revoked During the Audit Period

CAs Within the Audit Sope										
Common Name	Subject	Issuer	Serial	Key Algorithm	Key Size	Sig. Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
CHT Trust TLS CA - G1	CN = CHT Trust TLS CA - G1 O = Chunghwa Telecom Co., Ltd. C = TW	CN = CHT TrustRoot CA - G1 O = Chunghwa Telecom Co., Ltd. C = TW	00d0ec5a 2243fbd0 5ab8949 6811896 123d	rsaEncryption	4096 bits	sha256WithRSAEncryption	Aug 25, 2025 06:52:14 GMT	Aug 25, 2028 15:59:59 GMT	c78d5d8daa e8214edb2f6 372f2b57820 f02bf861	D242A4ABC87EABB 34E34C09E28F93FA 5D2764D047384A9 606E958C27A14115 BE



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 and locations in Scope, TLS Baseline

CP/CPS In-Scope

Document Name	Version	Effective Date
<u>HiPKICA CP/CPS</u>	1.1	2026-03-06
<u>HiPKICA CP/CPS</u>	1.05	2025-08-25

Locations In-Scope

CA Locations
Taipei, Taiwan
Taichung, Taiwan

MANAGEMENT'S ASSERTION OF CHUNGHWA TELECOM

Chunghwa Telecom Co., Ltd. (CHT) operates the Certification Authority (CA) services known as CAs in Appendix A and provides TLS CA services.

The management of CHT is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure on its website, CA business practices management, CA environmental controls, CA key lifecycle management controls, subscriber key lifecycle management controls, certificate lifecycle management controls, and subordinate CA 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 Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

CHT management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in CHT management's opinion, in providing its TLS services at locations as enumerated in Appendix B, throughout the period 26 October 2025 to 31 May 2026, CHT has:

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

including its commitment to provide TLS certificates in conformity with the CA/Browser Forum Requirements on the CHT website, and provided such services in accordance with its disclosed practices

- maintained effective controls to provide reasonable assurance that:
 - the integrity of keys and TLS certificates it manages is established and protected throughout their lifecycles; and
 - TLS certificate subscriber information is properly authenticated
- 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 – TLS Baseline v2.9.

CHT has disclosed the following matters publicly on Mozilla's Bugzilla platform:

Bug ID	Description	Date Opened	Date Closed
<u>2005567</u>	Chunghwa Telecom: CA Certificates Published in PEM format	2025-12-12	2026-02-03
<u>2005762</u>	Chunghwa Telecom: Failure to respond to CPR within 24 hours	2025-12-12	2026-02-05
<u>2008260</u>	Chunghwa Telecom: Delayed audit disclosure for GTLSCA	2026-01-01	2026-02-20
<u>2008782</u>	Chunghwa Telecom: Findings in 2025 WebTrust Audit - GTLSCA Audit Incident Report #1 - mass certificate revocation plan	2026-01-07	2026-02-18
<u>2008788</u>	Chunghwa Telecom: Findings in 2025 WebTrust Audit - GTLSCA Audit Incident Report #2 - Domain validation records without the TLS BR version	2026-01-07	2026-02-11

<u>2008799</u>	Chunghwa Telecom: Findings in 2025 WebTrust Audit - GTLSCA Audit Incident Report #3 - Missing vulnerability scan	2026-01-07	2026-02-20
<u>2008803</u>	Chunghwa Telecom: Findings in 2025 WebTrust Audit - GTLSCA Audit Incident Report #4 - Missing evaluation for third parties	2026-01-07	2026-02-13
<u>2009043</u>	Chunghwa Telecom: Delayed disclosure to Bug 2008782 GTLSCA Audit Incident Report #1 - mass certificate revocation plan	2026-01-08	2026-02-20
<u>2009045</u>	Chunghwa Telecom: Delayed disclosure to Bug 2008788 GTLSCA Audit Incident Report #2 - Domain validation records without the TLS BR version	2026-01-08	2026-02-20
<u>2009046</u>	Chunghwa Telecom: Delayed disclosure to Bug 2008799 GTLSCA Audit Incident Report #3 - Missing vulnerability scan	2026-01-08	2026-02-20
<u>2009048</u>	Chunghwa Telecom: Delayed disclosure to Bug 2008803 GTLSCA Audit Incident Report #4 - Missing evaluation for third parties	2026-01-08	2026-02-20
<u>2012274</u>	Chunghwa Telecom: Issuance of certificate using keys previously reported as compromised	2026-01-24	2026-03-09
<u>2025231</u>	Chunghwa Telecom: Test Website certificate not revoked	2026-03-23	2026-04-25

Signature: Quen-Zong Wu

Title: Vice President

August 10, 2026

Appendix A-List of CAs in Scope(TLS Baseline)

Root CAs										
Common Name	Subject	Issuer	Serial	Key Algorithm	Key Size	Sig. Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
CHT TrustRoot CA - G1	CN=CHT TrustRoot CA - G1, O=Chunghwa Telecom Co., Ltd., C=TW	CN=CHT TrustRoot CA - G1, O=Chunghwa Telecom Co., Ltd., C=TW	00e9bd907dc13595ccbe590fa5d39e572a	rsaEncryption	4096 bits	sha256WithRSAEncryption	Aug 25 06:42:38 2025 GMT	Aug 25 15:59:59 2040 GMT	a48b5449e90eb52a03ac16256ca6d101c9bd61ef	AC0B9F8E3F88C9BA1FACA0B360B6EC3DE1E2C7BE0EB508C063649ABA02061D39

OV TLS Issuing CA										
Common Name	Subject	Issuer	Serial	Key Algorithm	Key Size	Sig. Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
CHT Trust TLS CA - G1	CN = CHT Trust TLS CA - G1 O = Chunghwa Telecom Co., Ltd. C = TW	CN = CHT TrustRoot CA - G1 O = Chunghwa Telecom Co., Ltd. C = TW	709f59d2919894b8cd84205dc7015184	rsaEncryption	4096 bits	sha256WithRSAEncryption	Mar 12, 2026 02:53:09 GM	Mar 10, 2029 15:59:59 GMT	c78d5d8daae8214edb2f6372f2b57820f02bf861	14E9217404AC6F4443A622F3061CF5FDF10D2C6F9448EB4A1A25026FED247311

Appendix A-1 Certificates of CAs Revoked During the Audit Period

CAs Within the Audit Sope										
Common Name	Subject	Issuer	Serial	Key Algorithm	Key Size	Sig. Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
CHT Trust TLS CA - G1	CN = CHT Trust TLS CA - G1 O = Chunghwa Telecom Co., Ltd. C = TW	CN = CHT TrustRoot CA - G1 O = Chunghwa Telecom Co., Ltd. C = TW	00d0ec5 a2243fb d05ab89 4968118 96123d	rsaEncryption	4096 bits	sha256WithRSAEncryption	Aug 25, 2025 06:52:14 GMT	Aug 25, 2028 15:59:59 GMT	c78d5d8da ae8214edb 2f6372f2b5 7820f02bf8 61	D242A4ABC87EA BB34E34C09E28 F93FA5D2764D0 47384A9606E958 C27A14115BE

Appendix B- Certificate Policy and Certification Practice Statement Versions in Scope and locations in Scope, TLS Baseline

CP/CPS In-Scope

Document Name	Version	Effective Date
<u>HiPKICA CP/CPS</u>	1.1	2026-03-06
<u>HiPKICA CP/CPS</u>	1.05	2025-08-25

Locations In-Scope

CA Locations
Taipei, Taiwan
Taichung, Taiwan