



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 1 June 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.

Basis for qualified opinion

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

Observation	Relevant WebTrust TLS Baseline Criteria
We noted that 8 certificates issued by HiPKI OV TLS CA - G1 with private keys previously revoked with reason code <i>keyCompromise</i>. (bug #2012274) This caused WebTrust Principles and Criteria for Certification Authorities - TLS Baseline Version 2.9 Criterion 2.17 not to be met.	2.17 The CA maintains controls to provide reasonable assurance that it rejects a certificate request if one or more of the following conditions are met: . The Key Pair does not meet the requirements set forth in Section 6.1.5 and/or Section 6.1.6; . There is clear evidence that the specific method used to generate the Private Key was flawed;



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

	. The CA is aware of a demonstrated or proven method that exposes the Applicant's Private Key to compromise; . The CA has previously been notified that the Applicant's Private Key has suffered a Key Compromise, using the provisions of Section 4.9.1.1CA's procedure for revocation request as described in Section 4.9.3 and Section 4.9.12; and . The Public Key corresponds to an industry-demonstrated weak Private Key. For requests submitted on or after November 15, 2024, at least the precautions from Section 6.1.1.3 SHALL be implemented.
--	--

Qualified Opinion

In our opinion, except for the matters described in the basis for qualified opinion section above, throughout the period 1 June 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 Matters

Without modifying our opinion, we noted the following other matters during our procedures and have considered the nature of these matters in our risk assessment and in determining the nature, timing, and extent of our procedures. This included performing procedures to understand the root cause disclosed by the CA, and if facts and circumstances noted in our examination agreed with what has been disclosed. We have also considered the procedures the CA has designed and noted if implemented properly and operated effectively, the controls would address the root cause. We did not perform any procedures subsequent to this report as to the effectiveness of the controls implemented.

Matter Topic	Matter Topic	Matter Description
1	Certificate request	CHT disclosed in Mozilla bug <u>#2012274</u> that a certificate was issued using keys previously reported as compromised.
2	Certificate revocation	CHT disclosed in Mozilla bug <u>#2025231</u> that a Test Website certificate was not revoked.

While the CHT's assertion notes all issues disclosed on Bugzilla through the audit period of this report, we have only noted those instances relevant to the CAs enumerated in Appendix A and applicable to the WebTrust Principles and Criteria for Certification Authorities – TLS Baseline v2.9.

We also note that during the audit period, Chunghwa Telecom revoked the GTLSCA-G1 CA certificate (Certificate Serial Number: 00 99 6d 5f e9 ad e1 6c dc 8e cd bf ed b1 4a 32 95) on April 23, 2026, as described in Chunghwa Telecom's assertion. Our procedures included verifying that the CA certificate was on the eCA-G2 Certificate Revocation List and that the revocation was publicly disclosed through the CA repository website. However, the GTLSCA-G1 CA was not within the scope of our audit. Our procedures with respect to this matter were limited to the CAs as enumerated in Appendix A.

Use of the Qualified Mark

CHT's use of the WebTrust for Certification Authorities – TLS Baseline Qualified Mark constitutes a symbolic representation of the contents of this report and it is not



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

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
ePKI Root Certification Authority	C=TW, O=Chunghwa Telecom Co., Ltd., OU=ePKI Root Certification Authority	C=TW, O=Chunghwa Telecom Co., Ltd., OU=ePKI Root Certification Authority	15c8bd65475c afb897005ee4 06d2bc9d	rsaEncryption	4096 bits	sha1WithRSAEncryption	Dec 20 02:31:27 2004 GMT	Dec 20 02:31:27 2034 GMT	1e0cf7b667f2e192260945c055392e773f424aa2	COA6F4DC63A24BFDCF54EF2A6A082A0A72DE35803E2FF5FF527AE5D87206DFD5
ePKI Root Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G2	00d6962ec10a 159312af8f63b cd444c95b	rsaEncryption	4096 bits	sha256WithRSAEncryption	Nov 17 08:23:42 2015 GMT	Dec 31 15:59:59 2037 GMT	725bbaaa7238ee259024b59422fa0988ca8b0afb	1E51942B84FD467BF77D1C89DA241C04254DC8F3EF4C22451FE7A89978BDCD4F



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

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	2dddac ce6297 94a143 e8b0cd 766a5e 60	rsaEncryption	4096 bits	sha256With RSAEncryption	Feb 22 09:46:04 2019 GMT	Dec 31 15:59:59 2037 GMT	f27717fa5 ea8fef63d 71d568bac 9460c38d8 afb0	F015CE3CC239B FEF064BE9F1D2 C417E1A0264A0 A94BE1F0C8D12 1864EB6949CC



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

Cross-Signed CA Certificates										
Common Name	Subject	Issuer	Serial	Key Algorithm	Key Size	Sig. Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
ePKI Root Certification Authority	C=TW, O=Chunghwa Telecom Co., Ltd., OU=ePKI Root Certification Authority	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G2	18907402b083ec8bce1994deafc0a1d7	rsaEncryption	4096 bits	sha256WithRSAEncryption	Nov 17 08:31:41 2015 GMT	Dec 20 02:31:27 2034 GMT	1e0cf7b667f2e192260945c055392e773f424aa2	B9C974DE139F6308D74CCC423C3BC0BDED5E7AB4AD738B304B50D429C42C3D66
ePKI Root Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., OU=ePKI Root Certification Authority	3beee0918e8886ad460fe8ae910c9cb a	rsaEncryption	4096 bits	sha256WithRSAEncryption	Nov 17 08:51:35 2015 GMT	Dec 20 02:31:27 2034 GMT	725bbaaa7238ee259024b59422fa0988ca8b0afb	64717250AF8B028DD8E5C0BAE4C9142C8B103532612BC487085FD3C319F9C067
ePKI Root Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., OU=ePKI Root Certification Authority	00afcd8d642c62d645067dc857fda8f15d	rsaEncryption	4096 bits	sha256WithRSAEncryption	Nov 17 08:51:35 2015 GMT	Dec 20 02:31:27 2034 GMT	725bbaaa7238ee259024b59422fa0988ca8b0afb	18467C4E64D586C844A44466DE5BA7A6D5969C7A92859A511C5FDAD75B03CDC E



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

Cross-Signed CA Certificates										
Common Name	Subject	Issuer	Serial	Key Algorithm	Key Size	Sig. Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
ePKI Root Certification Authority - G2	CN = ePKI Root Certification Authority - G2 O = Chunghwa Telecom Co., Ltd. C = TW	OU = ePKI Root Certification Authority O = Chunghwa Telecom Co., Ltd. C = TW	00edb8f46f99dd6a9aad7623e3f2c11d05c	rsaEncryption	4096 bits	sha256WithRSAEncryption	Nov 17 08:51:35 2015 GMT	Dec 20 02:31:27 2034 GMT	725bbaaa7238ee259024b59422fa0988ca8b0afb	72D716F7BB6BD105704F42B9524923510DCB85B2D870C0E9ADB5AEB9C969051A
HiPKI Root CA - G1	CN = HiPKI Root CA - G1 O = Chunghwa Telecom Co., Ltd. C = TW	OU = ePKI Root Certification Authority O = Chunghwa Telecom Co., Ltd. C = TW	23fba648360e15e92ba78aedb67a0ae5	rsaEncryption	4096 bits	sha256WithRSAEncryption	Dec 21 02:11:23 2023 GMT	Dec 19 15:59:59 2034 GMT	f27717fa5ea8fef63d71d568bac9460c38d8afb0	6807C97235C5EC6090269A4B5FEDFAB46986E42F4D67D2EDDDCF6E45CF0DFA80



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

OV TLS Issuing CA										
Common Name	Subject	Issuer	Serial	Key Algorithm	Key Size	Sig. Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
Public Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., OU=Public Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., OU=ePKI Root Certification Authority	00c423d22191868fac4ee2fce4a011d1a7	rsaEncryption	2048 bits	sha256WithRSAEncryption	Dec 11 08:51:59 2014 GMT	Dec 11 08:51:59 2034 GMT	cb837d6515afa9c9f3a8a9f4647c795205744061	609930EB807AD420AFDA2A8AA61B67483039168CD766E09942A48BFE7F3BDC10
HiPKI OV TLS CA - G1	CN=HiPKI OV TLS CA - G1, O=Chunghwa Telecom Co., Ltd., C=TW	CN=HiPKI Root CA - G1, O=Chunghwa Telecom Co., Ltd., C=TW	2baba2d6e680cca594e04809af065d42	rsaEncryption	4096 bits	sha256WithRSAEncryption	May 18 02:51:28 2023 GMT	Dec 31 15:59:59 2037 GMT	358fc22e88de3313db0e2163ce542eb6824ca583	D34A5B981A85CA075DB62CBA C415EF659D95339040CA476868625D4AA23A9849



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
ePKI Root Certification Authority	C=TW, O=Chunghwa Telecom Co., Ltd., OU=ePKI Root Certification Authority	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G2	00cae1f73efcac5bb19c88c1c72f6f7b2f	rsaEncryption	4096 bits	sha256WithRSAEncryption	Nov 17 08:31:41 2015 GMT	Dec 20 02:31:27 2034 GMT	1e0cf7b667f2e192260945c055392e773f424aa2	D108C34A58C0E4A616449F8C48318023A229C86CD3DDD5D5FE6041A401C16A14
Public Certification Authority	C=TW, O=Chunghwa Telecom Co., Ltd., OU=Public Certification Authority	C=TW, O=Chunghwa Telecom Co., Ltd., OU=ePKI Root Certification Authority	00c953fee8b895e91884abb22a68a42a7d	rsaEncryption	2048 bits	sha1WithRSAEncryption	May 16 10:13:55 2007 GMT	May 16 10:13:55 2027 GMT	71b35031a01b5b7bb2a6597cfd108c3cad3a3d7a	464B0EC0A602F0193DB5F33911885A3A61921AD16D2664E25BEFAB10CFA6ED25



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

CAs Within the Audit Sope										
Common Name	Subject	Issuer	Serial	Key Algorithm	Key Size	Sig. Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
Public Certification Authority	C=TW, O=Chunghwa Telecom Co., Ltd., OU=Public Certification Authority	C=TW, O=Chunghwa Telecom Co., Ltd., OU=ePKI Root Certification Authority	00973c c94d44 cfe9a2e 14f52e 9a594a 15a	rsaEncryption	2048 bits	sha1WithRSAEncryption	May 16 10:13:55 2007 GMT	May 16 10:13:55 2027 GMT	71b35031 a01b5b7b b2a6597cf d108c3cad 3a3d7a	4BD16F4955F3F 3C9C8EA48EF99 95324DA512172 4F89915D5F2C9 1EB0BAEF2337

CA out of the Audit Sope										
Common Name	Subject	Issuer	Serial	Key Algorithm	Key Size	Sig. Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
政府伺服器數位憑證管理中心 - G1	CN = 政府伺服器數位憑證管理中心 - G1 O = 行政院 C = TW	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G2	00996d 5fe9ade 16cdc8 ecdbfed b14a32 95	rsaEncryption	4096 bits	sha256WithRSAEncryption	Jul 19 06:46:45 2019 GMT	Aug 19 06:46:45 2031 GMT	d6eb2d9d 61fe2bbb7 0882eb80 7b159b0f4 83226a	9D1CDA1B9EF3 95AFCE7DE0FE7 4DE6D9FF5E0D2 A43789116C00C 6BA5BF44B9823



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>ePKI CP</u>	2.3	2025-08-18
<u>ePKI CP</u>	2.2	2024-08-26
<u>CHTCA CPS</u>	1.4	2026-04-21
<u>CHTCA CPS</u>	1.3	2025-10-29
<u>CHTCA CPS</u>	1.2	2025-05-19
<u>HiPKICA CP/CPS</u>	1.1	2026-03-06
<u>HiPKICA CP/CPS</u>	1.05	2025-08-25
<u>HiPKICA CP/CPS</u>	1.0	2025-08-18
<u>HiPKICA CPS</u>	1.1	2025-05-19
<u>HiPKI CP</u>	1.3	2024-08-26

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. During our assessment, we noted the following observations which caused the relevant criteria to not be met:

Observation	Relevant WebTrust TLS Baseline Criteria
We noted that 8 certificates issued by HiPKI OV TLS CA - G1 with private keys previously revoked with reason code <i>keyCompromise</i> . This caused WebTrust Principles and Criteria for Certification Authorities - TLS Baseline Version	2.17 The CA maintains controls to provide reasonable assurance that it rejects a certificate request if one or more of the following conditions are met: . The Key Pair does not meet the requirements set forth in Section 6.1.5 and/or Section 6.1.6;

Observation	Relevant WebTrust TLS Baseline Criteria
2.9 Criterion 2.17 not to be met.	. There is clear evidence that the specific method used to generate the Private Key was flawed; . The CA is aware of a demonstrated or proven method that exposes the Applicant's Private Key to compromise; . The CA has previously been notified that the Applicant's Private Key has suffered a Key Compromise, using the provisions of Section 4.9.1.1CA's procedure for revocation request as described in Section 4.9.3 and Section 4.9.12; and . The Public Key corresponds to an industry-demonstrated weak Private Key. For requests submitted on or after November 15, 2024, at least the precautions from Section 6.1.1.3 SHALL be implemented.

Based on that assessment, in CHT management's opinion, except for the matters described in the preceding table, in providing its TLS services at locations as enumerated in Appendix B, throughout the period 1 June 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

Bug ID	Description	Date Opened	Date Closed
<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

During the audit period, Chunghwa Telecom revoked the GTLSCA-G1 CA certificate (Certificate Serial Number: 00 99 6d 5f e9 ad e1 6c dc 8e cd bf ed b1 4a 32 95), which was issued by ePKI Root Certification Authority - G2, on April 23, 2026. The CA was originally established to support TLS certificate services for the Ministry of Digital Affairs (MODA). Following the expiration of the related service contract and confirmation that continued operation was no longer required, the CA certificate was revoked and the revocation was publicly disclosed through the CA repository website.

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
ePKI Root Certification Authority	C=TW, O=Chunghwa Telecom Co., Ltd., OU=ePKI Root Certification Authority	C=TW, O=Chunghwa Telecom Co., Ltd., OU=ePKI Root Certification Authority	15c8bd65475cafb897005ee406d2bc9d	rsaEncryption	4096 bits	sha1WithRSAEncryption	Dec 20 02:31:27 2004 GMT	Dec 20 02:31:27 2034 GMT	1e0cf7b667f2e192260945c055392e773f424aa2	C0A6F4DC63A24BFDCF54EF2A6A082A0A72DE35803E2FF5FF527AE5D87206DFD5
ePKI Root Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G2	00d6962ec10a159312af8f63bcd44c95b	rsaEncryption	4096 bits	sha256WithRSAEncryption	Nov 17 08:23:42 2015 GMT	Dec 31 15:59:59 2037 GMT	725bbaaa7238ee259024b59422fa0988ca8b0afb	1E51942B84FD467BF77D1C89DA241C04254DC8F3EF4C22451FE7A89978BD4F
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	2dddacce629794a143e8b0c	rsaEncryption	4096 bits	sha256WithRSAEncryption	Feb 22 09:46:04 2019 GMT	Dec 31 15:59:59 2037 GMT	f27717fa5ea8fef63d71d568bac9460c38d8afb0	F015CE3CC239BFEF064BE9F1D2C417E1A0264A0A94BE

Root CAs										
Common Name	Subject	Issuer	Serial	Key Algorithm	Key Size	Sig. Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
			d766a5e60							1F0C8D121864EB6949CC

Cross-Signed CA Certificates										
Common Name	Subject	Issuer	Serial	Key Algorithm	Key Size	Sig. Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
ePKI Root Certification Authority	C=TW, O=Chunghwa Telecom Co., Ltd., OU=ePKI Root Certification Authority	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G2	18907402b083ec8bce1994deafc0a1d7	rsaEncryption	4096 bits	sha256WithRSAEncryption	Nov 17 08:31:41 2015 GMT	Dec 20 02:31:27 2034 GMT	1e0cf7b667f2e192260945c055392e773f424aa2	B9C974DE139F6308D74CCC423C3BC0BDED5E7AB4AD738B304B50D429C42C3D66
ePKI Root Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., OU=ePKI Root Certification Authority	3beee0918e8886ad460fe8ae910c9cba	rsaEncryption	4096 bits	sha256WithRSAEncryption	Nov 17 08:51:35 2015 GMT	Dec 20 02:31:27 2034 GMT	725bbaaa7238ee259024b59422fa0988ca8b0afb	64717250AF8B028DD8E5C0BAE4C9142C8B103532612BC487085FD3C319F9C067
ePKI Root Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., OU=ePKI Root Certification Authority	00afcd8d642c62d645067dc857fda8f15d	rsaEncryption	4096 bits	sha256WithRSAEncryption	Nov 17 08:51:35 2015 GMT	Dec 20 02:31:27 2034 GMT	725bbaaa7238ee259024b59422fa0988ca8b0afb	18467C4E64D586C844A44466DE5BA7A6D5969C7A92859A511C5FDA D75B03CDCE

Cross-Signed CA Certificates										
Common Name	Subject	Issuer	Serial	Key Algorithm	Key Size	Sig. Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
ePKI Root Certification Authority - G2	CN = ePKI Root Certification Authority - G2 O = Chunghwa Telecom Co., Ltd. C = TW	OU = ePKI Root Certification Authority O = Chunghwa Telecom Co., Ltd. C = TW	00edb8f46f99dd6a9aa7623e3f2c11d05c	rsaEncryption	4096 bits	sha256WithRSAEncryption	Nov 17 08:51:35 2015 GMT	Dec 20 02:31:27 2034 GMT	725bbaaa7238ee259024b59422fa0988ca8b0afb	72D716F7BB6BD105704F42B9524923510DCB85B2D870C0E9ADA5AEB9C969051A
HiPKI Root CA - G1	CN = HiPKI Root CA - G1 O = Chunghwa Telecom Co., Ltd. C = TW	OU = ePKI Root Certification Authority O = Chunghwa Telecom Co., Ltd. C = TW	23fba648360e15e92ba78aedb67a0ae5	rsaEncryption	4096 bits	sha256WithRSAEncryption	Dec 21 02:11:23 2023 GMT	Dec 19 15:59:59 2034 GMT	f27717fa5ea8fef63d71d568bac9460c38d8afb0	6807C97235C5EC6090269A4B5FEDFAB46986E42F4D67D2EDDDCF6E45CF0DFA80

OV TLS Issuing CA										
Common Name	Subject	Issuer	Serial	Key Algorithm	Key Size	Sig. Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
Public Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., OU=Public Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., OU=ePKI Root Certification Authority	00c423d22191868fac4ee2fce4a01d1a7	rsaEncryption	2048 bits	sha256WithRSAEncryption	Dec 11 08:51:59 2014 GMT	Dec 11 08:51:59 2034 GMT	cb837d6515afa9c9f3a8a9f4647c795205744061	609930EB807AD420AFDA2A8AA61B67483039168CD766E09942A48BFE7F3BDC10
HiPKI OV TLS CA - G1	CN=HiPKI OV TLS CA - G1, O=Chunghwa Telecom Co., Ltd., C=TW	CN=HiPKI Root CA - G1, O=Chunghwa Telecom Co., Ltd., C=TW	2baba2d6e680cca594e04809af065d42	rsaEncryption	4096 bits	sha256WithRSAEncryption	May 18 02:51:28 2023 GMT	Dec 31 15:59:59 2037 GMT	358fc22e88de3313db0e2163ce542eb6824ca583	D34A5B981A85CA075DB62CBAC415EF659D95339040CA476868625D4AA23A9849

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

CAs Within the Audit Scope										
Common Name	Subject	Issuer	Serial	Key Algorithm	Key Size	Sig. Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
ePKI Root Certification Authority	C=TW, O=Chunghwa Telecom Co., Ltd., OU=ePKI Root Certification Authority	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G2	00cae1f73efca5bb19c88c1c72f6f7b2f	rsaEncryption	4096 bits	sha256WithRSAEncryption	Nov 17 08:31:41 2015 GMT	Dec 20 02:31:27 2034 GMT	1e0cf7b667f2e192260945c055392e773f424aa2	D108C34A58C0E4A616449F8C48318023A229C86CD3DD5D5FE6041A401C16A14
Public Certification Authority	C=TW, O=Chunghwa Telecom Co., Ltd., OU=Public Certification Authority	C=TW, O=Chunghwa Telecom Co., Ltd., OU=ePKI Root Certification Authority	00c953feeb895e91884abb22a68a42a7d	rsaEncryption	2048 bits	sha1WithRSAEncryption	May 16 10:13:55 2007 GMT	May 16 10:13:55 2027 GMT	71b35031a01b5b7bb2a6597cfd108c3cad3a3d7a	464B0EC0A602F0193DB5F33911885A3A61921AD16D2664E25BEFAB10CFA6ED25

CAs Within the Audit Sope

Common Name	Subject	Issuer	Serial	Key Algorithm	Key Size	Sig. Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
Public Certification Authority	C=TW, O=Chunghwa Telecom Co., Ltd., OU=Public Certification Authority	C=TW, O=Chunghwa Telecom Co., Ltd., OU=ePKI Root Certification Authority	00973c c94d44 cfe9a2 e14f52 e9a59 4a15a	rsaEncryption	2048 bits	sha1WithRSAEncryption	May 16 10:13:55 2007 GMT	May 16 10:13:55 2027 GMT	71b35031 a01b5b7b b2a6597c fd108c3c ad3a3d7a	4BD16F4955F3F3C9C8EA48EF9995324DA5121724F89915D5F2C91EB0BAEF2337

CA out of the Audit Sope

Common Name	Subject	Issuer	Serial	Key Algorithm	Key Size	Sig. Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
政府伺服器數位憑證管理中心 - G1	CN = 政府伺服器數位憑證管理中心 - G1 O = 行政院 C = TW	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G2	00996 d5fe9a de16cd c8ecdb fedb14 a3295	rsaEncryption	4096 bits	sha256WithRSAEncryption	Jul 19 06:46:45 2019 GMT	Aug 19 06:46:45 2031 GMT	d6eb2d9d 61fe2bbb 70882eb8 07b159b0 f483226a	9D1CDA1B9EF395AFCE7DE0FE74DE6D9FF5E0D2A43789116C00C6BA5BF44B9823

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>ePKI CP</u>	2.3	2025-08-18
<u>ePKI CP</u>	2.2	2024-08-26
<u>CHTCA CPS</u>	1.4	2026-04-21
<u>CHTCA CPS</u>	1.3	2025-10-29
<u>CHTCA CPS</u>	1.2	2025-05-19
<u>HiPKICA CP/CPS</u>	1.1	2026-03-06
<u>HiPKICA CP/CPS</u>	1.05	2025-08-25
<u>HiPKICA CP/CPS</u>	1.0	2025-08-18
<u>HiPKICA CPS</u>	1.1	2025-05-19
<u>HiPKI CP</u>	1.3	2024-08-26

Locations In-Scope

CA Locations
Taipei, Taiwan
Taichung, Taiwan