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 Taipei and Taichung, Taiwan, throughout the period 1 June 2024 to 31 May 2025 for its CAs as enumerated in Appendix A, CHT has:

- disclosed its SSL 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 SSL 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 SSL certificates it manages is established and protected throughout their lifecycles; and
    - SSL 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 – SSL Baseline v2.8.

Certification authority's responsibilities

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

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 – SSL Baseline v2.8.

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, 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 SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of SSL certificates, and obtaining an understanding of CHT'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 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.

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

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 1 June 2024 to 31 May 2025, 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 – SSL Baseline v2.8.

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 – SSL Baseline v2.8, nor the suitability of any of CHT's services for any customer's intended purpose.

Other Matters

Without modifying our opinion, we noted the following other matters during our procedure:

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

Matter Topic		Matter Description
1	Publication of information	CHT disclosed in Mozilla bug #1904038 that "Test Website - Valid" URL (good.epkiov.hinet.net) disclosed to CCADB expired for 278 days, resulting in non-compliance with the TLS BR Section 2.2 and Root Program policies. CHT disclosed in Mozilla bug #1947034 that stale policy documents were disclosed to the CCADB.
2	Verification of Subject Identity information	CHT disclosed in Mozilla bug #1951415 that during the migration of the existing TLS certificates in GTLSCA to the HiPKI OV TLS CA, CHT recognize the evidences of domain control of these valid certificates on GTLSCA by reusing validation data or documents, and directly proceed with certificate reissuance through HiPKI OV TLS CA due to the fact that both GTLSCA and HiPKI OV TLS CA are operated by CHT without thoroughly checking the CAA records.
3	Certificate revocation	CHT disclosed in Mozilla bug #1959278 that 11,860 TLS certificates were planned to be revoked but 4 certificates were not revoked within the 24-hour period specified in TLS BR 4.9.1.1.
4	Delayed Annual Audit Report	CHT disclosed in Mozilla bug #1917224 that CHT did not upload audit reports to CCADB within 3 months after the end date of the annual audit period.
5	Root CA Lifecycles	Mozilla announced in Mozilla bug #1967548 that it would turn off the trust bit for the Chunghwa Telecom ePKI Root in Firefox 141, because the key material for the ePKI Root Certification Authority was created before 2006.

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

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

enumerated in Attachment A and applicable to the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline v2.8.

As set out in CCADB Public and Google Security Blog, we noted that Google publicly announced on May 30, 2025, its removal of default trust of CHT effective August 1, 2025. As part of our examination, we performed additional audit procedures regarding the aforementioned incidents. Based on our examination, we determined that the corrective actions, including the technical controls such as MPIC, ACME and PKILint were effectively implemented and operating during the period.

Use of the WebTrust seal

CHT's use of the WebTrust for Certification Authorities – SSL 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 8, 2025

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(BR)

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	00d6962ec10a159312af8f63bcd444c95b	rsaEncryption	4096 bits	sha256WithRSAEncryption	Nov 17 08:23:42 2015 GMT	Dec 31 15:59:59 2037 GMT	725bbaaa7238ee259024b59422fa0988ca8b0afb	1E51942B84FD467BF77D1C89DA241C04254DC8F3EF4C22451FE7A89978BDCD4F
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

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	00cae1f73efcac5bb19c88c1c72f6f7b2f	rsaEncryption	4096 bits	sha256WithRSAEncryption	Nov 17 08:31:41 2015 GMT	Dec 20 02:31:27 2034 GMT	1e0cf7b667f2e192260945c055392e773f424aa2	D108C34A58C0E4A616449F8C48318023A229C86CD3DDD5D5FE6041A401C16A14
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	C=TW, O=Chunghwa Telecom Co., Ltd., OU=ePKI Root	00afcd8d642c62d645067d	rsaEncryption	4096 bits	sha256WithRSAEncryption	Nov 17 08:51:35 2015 GMT	Dec 20 02:31:27 2034 GMT	725bbaaa7238ee259024	18467C4E64D586C844A44466DE5BA7A6D5969C7A92859

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**
	Certification Authority - G2	Certification Authority	c857fda8f15d						b59422fa0988ca8b0afb	A511C5FDAD75B03CDCE
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

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	C=TW, O=Chunghwa Telecom Co., Ltd., OU=Public Certification Authority	C=TW, O=Chunghwa Telecom Co., Ltd., OU=ePKI Root Certification Authority	00c953feeeb895e91884abb22a68a42a7d	rsaEncryption	2048 bits	sha1WithRSAEncryption	May 16 10:13:55 2007 GMT	May 16 10:13:55 2027 GMT	71b35031a01b5b7bb2a6597cfd108c3cad3a3d7a	464B0EC0A602F0193DB5F33911885A3A61921AD16D2664E25BEFAB10CFA6ED25
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	00973cc94d44cfe9a2e14f52e9a594a15a	rsaEncryption	2048 bits	sha1WithRSAEncryption	May 16 10:13:55 2007 GMT	May 16 10:13:55 2027 GMT	71b35031a01b5b7bb2a6597cfd108c3cad3a3d7a	4BD16F4955F3F3C9C8EA48EF9995324DA5121724F89915D5F2C91EB0BAEF2337
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
Public Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., OU=Public	C=TW, O=Chunghwa Telecom Co., Ltd., OU=ePKI Root	143596f2441a7167983ffc9	rsaEncryption	2048 bits	sha256WithRSAEncryption	Dec 11 08:51:59 2014 GMT	Dec 11 08:51:59 2034 GMT	cb837d6515afa9c9f3a8a9f4647c795205744061	DAE3434F696FC9F0F652E1B2A6F69B5E9273D09F43BD3BD

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**
	Certification Authority - G2	Certification Authority	597419b53							D4717D6141F8CD2C2
Public Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., OU=Public Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G2	00ce6097fd33e12da075cedc965dc0c4a3	rsaEncryption	2048 bits	sha256WithRSAEncryption	Dec 11 08:51:59 2014 GMT	Dec 11 08:51:59 2034 GMT	cb837d6515afa9c9f3a8a9f4647c795205744061	F5FB67C8453EDA34DBEC8A766574F07A03548C084AF2F5E6455EA769608D9AD5
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

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-List of CA Certificates issued During the Audit Period

N/A

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.2-List of CA Certificates Revoked During the Audit Period

N/A

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, BR

Document Name	Version	Effective Date
ePKI CP	2.2	2024-08-26
ePKI CP	2.1	2023-08-29
CHTCA CPS	1.2	2025-05-19
CHTCA CPS	1.1	2024-08-27
CHTCA CPS	1.07	2024-05-06
HiPKI CP	1.3	2024-08-26
HiPKI CP	1.2	2023-08-29
HiPKICA CPS	1.1	2025-05-19
HiPKICA CPS	1.0	2024-08-27
HiPKICA CPS	0.97	2024-05-06

中華電信

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 SSL CA services.

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 SSL CA services at Taipei and Taichung, Taiwan, throughout the period 1 June 2024 to 31 May 2025, CHT has:

- disclosed its SSL 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 SSL 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 SSL certificates it manages is established and protected throughout their lifecycles; and
  - SSL 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 – SSL Baseline v2.8.

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

Bug ID	Description	Date Opened	Date Closed
#1904038	"Test Website - Valid" URL disclosed to CCADB is expired	2024-06-21	2025-04-18
#1917224	Delayed Annual Audit Report 2024	2024-09-06	2024-12-05
#1947034	Outdated and stale policy documents disclosed to the CCADB	2025-02-09	2025-04-11
#1951415	Failure to check restrictive CAA record during Migration	2025-03-03	2025-05-28
# 1956910	OV TLS Server certificate issuance by GTLSCA without proper validation	2025-03-27	2025-05-22
#1959278	Delayed revocation for bug 1951415	2025-04-08	2025-06-10
#1967548	Turn off Websites Trust Bit for Chunghwa Telecom ePKI Root in FF 141	2025-05-20	2025-06-16

Signature: Quen-Zong Wu

Title: Vice President

August 8, 2025

中華電信

Appendix A-List of CAs in Scope(BR)

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	00d6962ec10a159312af8f63bcd444c95b	rsaEncryption	4096 bits	sha256WithRSAEncryption	Nov 17 08:23:42 2015 GMT	Dec 31 15:59:59 2037 GMT	725bbaaa7238ee259024b59422fa0988ca8b0afb	1E51942B84FD467BF77D1C89DA241C04254DC8F3EF4C22451FE7A89978BDCD4F
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

中華電信

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	00cae1f73efcac5bb19c88c1c72f6f7b2f	rsaEncryption	4096 bits	sha256WithRSAEncryption	Nov 17 08:31:41 2015 GMT	Dec 20 02:31:27 2034 GMT	1e0cf7b667f2e192260945c055392e773f424aa2	D108C34A58C0E4A616449F8C48318023A229C86CD3DDD5D5FE6041A401C16A14
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	18467C4E64D586C844A44466DE5BA7A6D5969C7A92859A511C5FDAD75B03CDCE

中華電信

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

中華電信

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	C=TW, O=Chunghwa Telecom Co., Ltd., OU=Public Certification Authority	C=TW, O=Chunghwa Telecom Co., Ltd., OU=ePKI Root Certification Authority	00c953feeeb895e91884abb22a68a42a7d	rsaEncryption	2048 bits	sha1WithRSAEncryption	May 16 10:13:55 2007 GMT	May 16 10:13:55 2027 GMT	71b35031a01b5b7bb2a6597cfd108c3cad3a3d7a	464B0EC0A602F0193DB5F33911885A3A61921AD16D2664E25BEFAB10CFA6ED25
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	00973cc94d44cfe9a2e14f52e9a594a15a	rsaEncryption	2048 bits	sha1WithRSAEncryption	May 16 10:13:55 2007 GMT	May 16 10:13:55 2027 GMT	71b35031a01b5b7bb2a6597cfd108c3cad3a3d7a	4BD16F4955F3F3C9C8EA48EF9995324DA5121724F89915D5F2C91EB0BAEF2337
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
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	143596f2441a7167983ffc9597419b53	rsaEncryption	2048 bits	sha256WithRSAEncryption	Dec 11 08:51:59 2014 GMT	Dec 11 08:51:59 2034 GMT	cb837d6515afa9c9f3a8a9f4647c795205744061	DAE3434F696FC9F0F652E1B2A6F69B5E9273D09F43BD3BDD4717D6141F8CD2C2

中華電信

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., CN=ePKI Root Certification Authority - G2	00ce6097fd33e12da075cedc965dc0c4a3	rsaEncryption	2048 bits	sha256WithRSAEncryption	Dec 11 08:51:59 2014 GMT	Dec 11 08:51:59 2034 GMT	cb837d6515afa9c9f3a8a9f4647c795205744061	F5FB67C8453EDA34DBEC8A766574F07A03548C084AF2F5E6455EA769608D9AD5
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-List of CA Certificates issued During the Audit Period

N/A

Appendix A.2-List of CA Certificates Revoked During the Audit Period

N/A

中華電信

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

Document Name	Version	Effective Date
ePKI CP	2.2	2024-08-26
ePKI CP	2.1	2023-08-29
CHTCA CPS	1.2	2025-05-19
CHTCA CPS	1.1	2024-08-27
CHTCA CPS	1.07	2024-05-06
HiPKI CP	1.3	2024-08-26
HiPKI CP	1.2	2023-08-29
HiPKICA CPS	1.1	2025-05-19
HiPKICA CPS	1.0	2024-08-27
HiPKICA CPS	0.97	2024-05-06