



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 2023 to 31 May 2024 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 and non-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
- 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.](#)



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

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 – 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 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



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 1 June 2023 to 31 May 2024, 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 with Network Security v2.7.

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 with Network Security v2.7, 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 for Certification Authorities – SSL Baseline with Network



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

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.



日盛聯合會計師事務所
SUN RISE CPAS' FIRM
DFK INTERNATIONAL

October 22, 2024

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	15c8bd6 5475cafb 897005e e406d2b c9d	rsaEncryption	4096 bits	sha1WithRSAEncryption	Dec 20 02:31:27 2004 GMT	Dec 20 02:31:27 2034 GMT	1e0cf7b667f 2e19226094 5c055392e7 73f424aa2	COA6F4DC63A24BF DCF54EF2A6A082A 0A72DE35803E2FF5 FF527AE5D87206D FD5
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	00d6962 ec10a159 312af8f6 3bcd444c 95b	rsaEncryption	4096 bits	sha256WithRSAEncryption	Nov 17 08:23:42 2015 GMT	Dec 31 15:59:59 2037 GMT	725bbaaa72 38ee259024 b59422fa098 8ca8b0afb	1E51942B84FD467 BF77D1C89DA241C 04254DC8F3EF4C22 451FE7A89978BDC D4F
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	2dddacce 629794a 143e8b0 cd766a5e 60	rsaEncryption	4096 bits	sha256WithRSAEncryption	Feb 22 09:46:04 2019 GMT	Dec 31 15:59:59 2037 GMT	f27717fa5ea 8fef63d71d5 68bac9460c3 8d8afb0	F015CE3CC239BFEF 064BE9F1D2C417E1 A0264A0A94BE1F0 C8D121864EB6949 CC



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	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	3beee09 18e8886 ad460fe8 ae910c9c ba	rsaEncryption	4096 bits	sha256WithRS AEncryption	Nov 17 08:51:35 2015 GMT	Dec 20 02:31:27 2034 GMT	725bbaaa72 38ee259024 b59422fa098 8ca8b0afb	64717250AF8B028 DD8E5C0BAE4C914 2C8B103532612BC 487085FD3C319F9C 067
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	00afcd8d 642c62d 645067d c857fda8 f15d	rsaEncryption	4096 bits	sha256WithRS AEncryption	Nov 17 08:51:35 2015 GMT	Dec 20 02:31:27 2034 GMT	725bbaaa72 38ee259024 b59422fa098 8ca8b0afb	18467C4E64D586C 844A44466DE5BA7 A6D5969C7A92859 A511C5FDAD75B03 CDCE
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	00edb8f4 6f99dd6a 9aa7623 e3f2c11d 05c	rsaEncryption	4096 bits	sha256WithRS AEncryption	Nov 17 08:51:35 2015 GMT	Dec 20 02:31:27 2034 GMT	725bbaaa72 38ee259024 b59422fa098 8ca8b0afb	72D716F7BB6BD10 5704F42B95249235 10DCB85B2D870C0 E9ADA5AEB9C9690 51A



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
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	23fba648 360e15e 92ba78a edb67a0 ae5	rsaEncryption	4096 bits	sha256WithRSAEncryption	Dec 21 02:11:23 2023 GMT	Dec 19 15:59:59 2034 GMT	f27717fa5ea 8fef63d71d5 68bac9460c3 8d8afb0	6807C97235C5EC60 90269A4B5FEDFAB 46986E42F4D67D2 EDDDCF6E45CF0DF A80



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	00c953fe eeb895e 91884ab b22a68a 42a7d	rsaEncryption	2048 bits	sha1WithRSAE ncryption	May 16 10:13:55 2007 GMT	May 16 10:13:55 2027 GMT	71b35031a0 1b5b7bb2a6 597cfd108c3 cad3a3d7a	464B0EC0A602F019 3DB5F33911885A3 A61921AD16D2664 E25BEFAB10CFA6E D25
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	00973cc9 4d44cfe9 a2e14f52 e9a594a 15a	rsaEncryption	2048 bits	sha1WithRSAE ncryption	May 16 10:13:55 2007 GMT	May 16 10:13:55 2027 GMT	71b35031a0 1b5b7bb2a6 597cfd108c3 cad3a3d7a	4BD16F4955F3F3C9 C8EA48EF9995324 DA5121724F89915 D5F2C91EB0BAEF2 337
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	00c423d 2219186 8fac4ee2 fce4a011 d1a7	rsaEncryption	2048 bits	sha256WithRS AEncryption	Dec 11 08:51:59 2014 GMT	Dec 11 08:51:59 2034 GMT	cb837d6515 afa9c9f3a8a 9f4647c7952 05744061	609930EB807AD42 0AFDA2A8AA61B67 483039168CD766E 09942A48BFE7F3B DC10
Public Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., OU=Public	C=TW, O=Chunghwa Telecom Co., Ltd., OU=ePKI Root	143596f2 441a716 7983ffc9	rsaEncryption	2048 bits	sha256WithRS AEncryption	Dec 11 08:51:59 2014 GMT	Dec 11 08:51:59 2034 GMT	cb837d6515 afa9c9f3a8a 9f4647c7952 05744061	DAE3434F696FC9F0 F652E1B2A6F69B5E 9273D09F43BD3BD



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	597419b 53							D4717D6141F8CD2 C2
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	00ce6097 fd33e12d a075cedc 965dc0c4 a3	rsaEncryption	2048 bits	sha256WithRS AEncryption	Dec 11 08:51:59 2014 GMT	Dec 11 08:51:59 2034 GMT	cb837d6515 afa9c9f3a8a 9f4647c7952 05744061	F5FB67C8453EDA3 4DBEC8A766574F0 7A03548C084AF2F5 E6455EA769608D9 AD5
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	2baba2d 6e680cca 594e048 09af065d 42	rsaEncryption	4096 bits	sha256WithRS AEncryption	May 18 02:51:28 2023 GMT	Dec 31 15:59:59 2037 GMT	358fc22e88d e3313db0e2 163ce542eb 6824ca583	D34A5B981A85CA0 75DB62CBAC415EF 659D95339040CA4 76868625D4AA23A 9849



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

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	00edb8f4 6f99dd6a 9aa7623 e3f2c11d 05c	rsaEncryption	4096 bits	sha256WithRSAEncryption	Nov 17 08:51:35 2015 GMT	Dec 20 02:31:27 2034 GMT	725bbaaa72 38ee259024 b59422fa098 8ca8b0afb	72D716F7BB6BD10 5704F42B95249235 10DCB85B2D870C0 E9ADA5AEB9C9690 51A
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	23fba648 360e15e 92ba78a edb67a0 ae5	rsaEncryption	4096 bits	sha256WithRSAEncryption	Dec 21 02:11:23 2023 GMT	Dec 19 15:59:59 2034 GMT	f27717fa5ea 8fef63d71d5 68bac9460c3 8d8afb0	6807C97235C5EC60 90269A4B5FEDFAB 46986E42F4D67D2 EDDDCF6E45CF0DF A80



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
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.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	V2.1	August 29, 2023
ePKI CP	V2.05	December 7, 2022
CHTCA CPS	V1.07	May 06, 2024
CHTCA CPS	V1.05	August 29, 2023
CHTCA CPS	V1.0	April 6, 2023
HiPKI CP	V1.2	August 29, 2023
HiPKI CP	V1.17	August 30, 2022
HiPKICA CPS	V0.97	May 06, 2024
HiPKI CA CPS	V0.95	May 12, 2023

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 and non-SSL CA services at Taipei and Taichung, Taiwan, throughout the period 1 June 2023 to 31 May 2024, 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
- 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.](#)

Signature: Quen-Zong Wu

Title: Vice President

October 22, 2024

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	C0A6F4DC63A24BF DCF54EF2A6A082A 0A72DE35803E2FF5 FF527AE5D87206D FD5
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	1E51942B84FD467 BF77D1C89DA241C 04254DC8F3EF4C22 451FE7A89978BDC D4F
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	F015CE3CC239BFEF 064BE9F1D2C417E1 A0264A0A94BE1F0 C8D121864EB6949 CC

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	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
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	23fba648360e15e92ba78aedb67a0ae5	rsaEncryption	4096 bits	sha256WithRSAEncryption	Dec 21 02:11:23 2023 GMT	Dec 19 15:59:59 2034 GMT	f27717fa5ea8fef63d71d568bac9460c38d8afb0	6807C97235C5EC6090269A4B5FEDFAB46986E42F4D67D2EDDDCF6E45CF0DFA80

Cross-Signed CA Certificates										
Common Name	Subject	Issuer	Serial	Key Algorithm	Key Size	Sig. Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
		Telecom Co., Ltd. C = TW								

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	00c953fe eeb895e 91884ab b22a68a 42a7d	rsaEncryption	2048 bits	sha1WithRSAE ncryption	May 16 10:13:55 2007 GMT	May 16 10:13:55 2027 GMT	71b35031a0 1b5b7bb2a6 597cfd108c3 cad3a3d7a	464B0EC0A602F019 3DB5F33911885A3 A61921AD16D2664 E25BEFAB10CFA6E D25
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	00973cc9 4d44cfe9 a2e14f52 e9a594a 15a	rsaEncryption	2048 bits	sha1WithRSAE ncryption	May 16 10:13:55 2007 GMT	May 16 10:13:55 2027 GMT	71b35031a0 1b5b7bb2a6 597cfd108c3 cad3a3d7a	4BD16F4955F3F3C9 C8EA48EF9995324 DA5121724F89915 D5F2C91EB0BAEF2 337
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	00c423d 2219186 8fac4ee2 fce4a011 d1a7	rsaEncryption	2048 bits	sha256WithRS AEncryption	Dec 11 08:51:59 2014 GMT	Dec 11 08:51:59 2034 GMT	cb837d6515 afa9c9f3a8a 9f4647c7952 05744061	609930EB807AD42 0AFDA2A8AA61B67 483039168CD766E 09942A48BFE7F3B DC10
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	143596f2 441a716 7983ffc9 597419b 53	rsaEncryption	2048 bits	sha256WithRS AEncryption	Dec 11 08:51:59 2014 GMT	Dec 11 08:51:59 2034 GMT	cb837d6515 afa9c9f3a8a 9f4647c7952 05744061	DAE3434F696FC9F0 F652E1B2A6F69B5E 9273D09F43BD3BD D4717D6141F8CD2 C2

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	00ce6097 fd33e12d a075cedc 965dc0c4 a3	rsaEncryption	2048 bits	sha256WithRS AEncryption	Dec 11 08:51:59 2014 GMT	Dec 11 08:51:59 2034 GMT	cb837d6515 afa9c9f3a8a 9f4647c7952 05744061	F5FB67C8453EDA3 4DBEC8A766574F0 7A03548C084AF2F5 E6455EA769608D9 AD5
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	2baba2d 6e680cca 594e048 09af065d 42	rsaEncryption	4096 bits	sha256WithRS AEncryption	May 18 02:51:28 2023 GMT	Dec 31 15:59:59 2037 GMT	358fc22e88d e3313db0e2 163ce542eb 6824ca583	D34A5B981A85CA0 75DB62CBAC415EF 659D95339040CA4 76868625D4AA23A 9849

Appendix A.1-List of CA Certificates issued During the Audit Period

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	00edb8f4 6f99dd6a 9aa7623 e3f2c11d 05c	rsaEncryption	4096 bits	sha256WithRSAEncryption	Nov 17 08:51:35 2015 GMT	Dec 20 02:31:27 2034 GMT	725bbaaa72 38ee259024 b59422fa098 8ca8b0afb	72D716F7BB6BD10 5704F42B95249235 10DCB85B2D870C0 E9ADA5AEB9C9690 51A
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	23fba648 360e15e 92ba78a edb67a0 ae5	rsaEncryption	4096 bits	sha256WithRSAEncryption	Dec 21 02:11:23 2023 GMT	Dec 19 15:59:59 2034 GMT	f27717fa5ea 8fef63d71d5 68bac9460c3 8d8afb0	6807C97235C5EC60 90269A4B5FEDFAB 46986E42F4D67D2 EDDDCF6E45CF0DF A80

OV TLS Issuing CA										
Common Name	Subject	Issuer	Serial	Key Algorithm	Key Size	Sig. Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
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.2-List of CA Certificates Revoked During the Audit Period

N/A

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

Document Name	Version	Effective Date
ePKI CP	V2.1	August 29, 2023
ePKI CP	V2.05	December 7, 2022
CHTCA CPS	V1.07	May 06, 2024
CHTCA CPS	V1.05	August 29, 2023
CHTCA CPS	V1.0	April 6, 2023
HiPKI CP	V1.2	August 29, 2023
HiPKI CP	V1.17	August 30, 2022
HiPKICA CPS	V0.97	May 06, 2024
HiPKI CA CPS	V0.95	May 12, 2023