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 business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in the applicable versions of its CHT Certification Practice Statement ("CPS") and CHT Certificate Policy ("CP") as enumerated in Appendix B

- maintained effective controls to provide reasonable assurance that:
  - CHT's CPS is consistent with its CP; and
  - CHT provides its services in accordance with its CP and CPS.
- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
  - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles; and
  - subscriber information is properly authenticated (for the registration activities performed by CHT)
  - subordinate CA certificate requests are accurate, authenticated, and approved

- 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

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

in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.2.2.

CHT does not escrow its CA keys. Accordingly, our procedures did not extend to controls that would address those criteria.

CHT makes use of external registration authorities for specific subscriber registration activities as disclosed in CHT's business practices. Our procedures did not extend to the controls exercised by these external registration authorities.

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 v2.2.2

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

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

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 key and certificate lifecycle management business practices and its controls over key and certificate integrity, over the authenticity and confidentiality of subscriber and relying party information, over the continuity of key and certificate lifecycle management operations and over development, maintenance and operation of systems integrity;
(2) selectively testing transactions executed in accordance with disclosed key and 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

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

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 v2.2.2.

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 v2.2.2, 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 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(WTCA)

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
ePKI Root Certification Authority - G3	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G3	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G3	6237e01b9aae4e4df86229bb44497b01	rsaEncryption	4096 bits	sha256WithRSAEncryption	Apr 30 09:42:34 2019 GMT	Dec 31 15:59:59 2037 GMT	51ce2e18aca1a4003549ba923bff095bbf3884ac	558FAB7F4B5DFF16B68BA4E40D1D3E940EFA9B013350617D6F377C1724D9D421

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
ePKI Root Certification Authority - G4	CN=ePKI Root Certification Authority - G4, O=Chunghwa Telecom Co., Ltd., C=TW	CN=ePKI Root Certification Authority - G4, O=Chunghwa Telecom Co., Ltd., C=TW	00f670f95988f452058e31e168863efa7a	rsaEncryption	4096 bits	sha256WithRSAEncryption	Nov 3 03:43:14 2022 GMT	Nov 3 15:59:59 2047 GMT	8dcf0a7c6f219db653aa46697cda3f756454a098	19A2FA09332C6D8EAC1393D5F30371DD8B4DD687B0E1E50A6B48AE762CABA2B5
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

Timestamp CA										
Common Name	**Subject**	**Issuer**	**Serial**	**Key Algorithm**	**Key Size**	**Sig. Algorithm**	**Not Before**	**Not After**	**SKI**	**SHA256 Fingerprint**
ePKI Timestamping CA - G1	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Timestamping CA - G1	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G2	00b2143 7d0d67c 6387484 4f8461c5 f4b54	rsaEncryption	4096 bits	sha256WithRSAEncryption	Oct 18 02:50:29 2019 GMT	Dec 29 16:00:00 2037 GMT	d696a2d596 6e2d3e40b1 a3b26d8877 7bf6d6f4ca	DA31293D659781C 69E0085C732A2811 DB50E5CC5769091 49B80A98A9B0F93 FD9

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

Secure Email (S/MIME) CA										
Common Name	Subject	Issuer	Serial	Key Algorithm	Key Size	Sig. Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
CHT SMIME CA - G1	C=TW, O=Chunghwa Telecom Co., Ltd., CN=CHT SMIME CA - G1	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G2	7239e9d901bcd196e3658d9277db3470	rsaEncryption	4096 bits	sha256WithRSAEncryption	Jan 7 03:11:12 2021 GMT	Dec 29 16:00:00 2037 GMT	e985e072080d3922821a46a707ec514198476b4a	5EB6CC7D03C349B2DCC5BDD7B10141FC7AB8AE1844944F6950BE741D3D731C95
CHT SMIME CA - G1	C=TW, O=Chunghwa Telecom Co., Ltd., CN=CHT SMIME CA - G1	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G2	3878d76c8139e415898a37345e514650	rsaEncryption	4096 bits	sha256WithRSAEncryption	Jan 7 03:11:12 2021 GMT	Dec 29 16:00:00 2037 GMT	e985e072080d3922821a46a707ec514198476b4a	4AB2728FEC2114769461A2F5C2F51322497C7B923A0D8153E238F2AB073E3C2F
CHT SMIME CA - G2	CN=CHT SMIME CA - G2, O=hunghwa Telecom Co., Ltd., C=TW	CN=ePKI Root Certification Authority - G4, O=Chunghwa Telecom Co., Ltd., C=TW	09d94ead4f0a926b3cc6387c3582eab5	rsaEncryption	4096 bits	sha256WithRSAEncryption	Dec 21 02:29:51 2023 GMT	Dec 21 15:59:59 2038 GMT	4f7a5ab61048388c1211515058075e240912390c	15DC43B3BDA29DF4546008A4FC306DE811F3E78D804E1B989C2DE11D5336DA1A

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

Document Signing & Adobe CA										
Common Name	**Subject**	**Issuer**	**Serial**	**Key Algorithm**	**Key Size**	**Sig. Algorithm**	**Not Before**	**Not After**	**SKI**	**SHA256 Fingerprint**
Public Certification Authority - G4	CN=Public Certification Authority - G4, O=Chunghwa Telecom Co., Ltd., C=TW	CN=ePKI Root Certification Authority - G4, O=Chunghwa Telecom Co., Ltd., C=TW	291c0c63c0172bb1259f5a425aaf24e3	rsaEncryption	4096 bits	sha256WithRSAEncryption	Nov 3 03:54:17 2022 GMT	Nov 3 15:59:59 2042 GMT	fe9a1c00b8c34bd0190d7592deca4fccccde7454	8FAF35AA59EBB971FB4FC6131DD9C2DA41C18421C86FDEC274606EC31EBE5436

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 CA										
Common Name	**Subject**	**Issuer**	**Serial**	**Key Algorithm**	**Key Size**	**Sig. Algorithm**	**Not Before**	**Not After**	**SKI**	**SHA256 Fingerprint**
Public Certification Authority - G3	C=TW, O=Chunghwa Telecom Co., Ltd., CN=Public Certification Authority - G3	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G3	0088c1807ba0abb62e1f49a42a028be43e	rsaEncryption	2048 bits	sha256WithRSAEncryption	Apr 30 09:52:26 2019 GMT	Dec 31 15:59:59 2037 GMT	7b6b4b5754a5bb5d1a081ee986ec203b3951287c	B0F1F7C7DF837BDF88825A444444E4815DA7E0899728A07AE8767D5F65B50995

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	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**
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

Secure Email (S/MIME) CA										
Common Name	**Subject**	**Issuer**	**Serial**	**Key Algorithm**	**Key Size**	**Sig. Algorithm**	**Not Before**	**Not After**	**SKI**	**SHA256 Fingerprint**
CHT SMIME CA - G1	C=TW, O=Chunghwa Telecom Co., Ltd., CN=CHT SMIME CA - G1	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G2	3878d76c8139e415898a37345e514650	rsaEncryption	4096 bits	sha256WithRSAEncryption	Jan 7 03:11:12 2021 GMT	Dec 29 16:00:00 2037 GMT	e985e072080d3922821a46a707ec514198476b4a	4AB2728FEC2114769461A2F5C2F51322497C7B923A0D8153E238F2AB073E3C2F

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

Secure Email (S/MIME) CA										
Common Name	**Subject**	**Issuer**	**Serial**	**Key Algorithm**	**Key Size**	**Sig. Algorithm**	**Not Before**	**Not After**	**SKI**	**SHA256 Fingerprint**
CHT SMIME CA - G2	CN=CHT SMIME CA - G2, O=hunghwa Telecom Co., Ltd., C=TW	CN=ePKI Root Certification Authority - G4, O=Chunghwa Telecom Co., Ltd., C=TW	09d94ea d4f0a926 b3cc6387 c3582eab 5	rsaEncryption	4096 bits	sha256WithRS AEncryption	Dec 21 02:29:51 2023 GMT	Dec 21 15:59:59 2038 GMT	4f7a5ab6104 8388c12115 15058075e2 40912390c	15DC43B3BDA29DF 4546008A4FC306D E811F3E78D804E1B 989C2DE11D5336D A1A

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, WTCA

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

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 the following CA services:

- Subscriber Key Generation Services
- Subscriber Registration
- Certificate Renewal
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Suspension
- Certificate Validation
- Integrated Circuit Card (ICC) Life Cycle Management
- Subordinate CA certification

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 CA services at Taipei and Taichung, Taiwan, throughout the period 1 June 2023 to 31 May 2024, CHT has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in the applicable versions of its CHT Certification Practice Statement ("CPS") and CHT Certificate Policy ("CP") as enumerated in Appendix B

- maintained effective controls to provide reasonable assurance that:
    - CHT's Certification Practice Statement is consistent with its Certificate Policy
    - CHT provides its services in accordance with its Certificate Policy and Certification Practice Statement

- maintained effective controls to provide reasonable assurance that:
    - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
    - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles; and
    - subscriber information is properly authenticated (for the registration activities performed by CHT)
    - Subordinate CA certificate requests are accurate, authenticated and approved

- 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 v2.2.2, including the following:

CA Business Practices Disclosure

- Certification Practice Statement (CPS)
- Certificate Policy (CP)

CA Business Practices Management

- Certificate Policy Management
- Certification Practice Statement Management
- CP and CPS Consistency

CA Environmental Controls

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical & Environmental Security
- Operations Management
- System Access Management
- System Development and Maintenance
- Business Continuity Management
- Monitoring and Compliance
- Audit Logging

CA Key Lifecycle Management Controls

- CA Key Generation
- CA Key Storage, Backup, and Recovery
- CA Public Key Distribution
- CA Key Usage
- CA Key Archival and Destruction
- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management

中華電信

Subscriber Key Lifecycle Management Controls

- CA-Provided Subscriber Key Generation Services
- Integrated Circuit Card (ICC) Lifecycle Management
- Requirements for Subscriber Key Management

Certificate Lifecycle Management Controls

- Subscriber Registration
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Suspension
- Certificate Revocation
- Certificate Validation

Subordinate CA Certificate Lifecycle Management Controls

- Subordinate CA Certificate Lifecycle Management

CHT does not escrow its CA keys for CAs. Accordingly, our assertion does not extend to controls that would address those criteria.

Signature: Quen-Zong Wu

Title: Vice President

October 22, 2024

中華電信

Appendix A-List of CAs in Scope(WTCA)

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
ePKI Root Certification Authority - G3	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G3	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G3	6237e01b9aae4e4df86229bb44497b01	rsaEncryption	4096 bits	sha256WithRSAEncryption	Apr 30 09:42:34 2019 GMT	Dec 31 15:59:59 2037 GMT	51ce2e18aca1a4003549ba923bff095bbf3884ac	558FAB7F4B5DFF16B68BA4E40D1D3E940EFA9B013350617D6F377C1724D9D421
ePKI Root Certification Authority - G4	CN=ePKI Root Certification Authority - G4, O=Chunghwa	CN=ePKI Root Certification Authority - G4, O=Chunghwa	00f670f95988f452058e31e168863efa7a	rsaEncryption	4096 bits	sha256WithRSAEncryption	Nov 3 03:43:14 2022 GMT	Nov 3 15:59:59 2047 GMT	8dcf0a7c6f219db653aa46697cda3f756454a098	19A2FA09332C6D8EAC1393D5F30371DD8B4DD687B0E1E50A6B48AE762CABA2B5

中華電信

Root CAs										
Common Name	Subject	Issuer	Serial	Key Algorithm	Key Size	Sig. Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
	Telecom Co., Ltd., C=TW	Telecom Co., Ltd., C=TW								
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

Timestamp CA										
Common Name	**Subject**	**Issuer**	**Serial**	**Key Algorithm**	**Key Size**	**Sig. Algorithm**	**Not Before**	**Not After**	**SKI**	**SHA256 Fingerprint**
ePKI Timestamping CA - G1	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Timestamping CA - G1	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G2	00b2143 7d0d67c 6387484 4f8461c5 f4b54	rsaEncryption	4096 bits	sha256WithRSAEncryption	Oct 18 02:50:29 2019 GMT	Dec 29 16:00:00 2037 GMT	d696a2d596 6e2d3e40b1 a3b26d8877 7bf6d6f4ca	DA31293D659781C 69E0085C732A2811 DB50E5CC5769091 49B80A98A9B0F93 FD9

中華電信

Secure Email (S/MIME) CA										
Common Name	Subject	Issuer	Serial	Key Algorithm	Key Size	Sig. Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
CHT SMIME CA - G1	C=TW, O=Chunghwa Telecom Co., Ltd., CN=CHT SMIME CA - G1	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G2	7239e9d901bcd196e3658d9277db3470	rsaEncryption	4096 bits	sha256WithRSAEncryption	Jan 7 03:11:12 2021 GMT	Dec 29 16:00:00 2037 GMT	e985e072080d3922821a46a707ec514198476b4a	5EB6CC7D03C349B2DCC5BDD7B10141FC7AB8AE1844944F6950BE741D3D731C95
CHT SMIME CA - G1	C=TW, O=Chunghwa Telecom Co., Ltd., CN=CHT SMIME CA - G1	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G2	3878d76c8139e415898a37345e514650	rsaEncryption	4096 bits	sha256WithRSAEncryption	Jan 7 03:11:12 2021 GMT	Dec 29 16:00:00 2037 GMT	e985e072080d3922821a46a707ec514198476b4a	4AB2728FEC2114769461A2F5C2F51322497C7B923A0D8153E238F2AB073E3C2F
CHT SMIME CA - G2	CN=CHT SMIME CA - G2, O=hunghwa Telecom Co., Ltd., C=TW	CN=ePKI Root Certification Authority - G4, O=Chunghwa Telecom Co., Ltd., C=TW	09d94ead4f0a926b3cc6387c3582eab5	rsaEncryption	4096 bits	sha256WithRSAEncryption	Dec 21 02:29:51 2023 GMT	Dec 21 15:59:59 2038 GMT	4f7a5ab61048388c1211515058075e240912390c	15DC43B3BDA29DF4546008A4FC306DE811F3E78D804E1B989C2DE11D5336DA1A

Document Signing & Adobe CA										
Common Name	**Subject**	**Issuer**	**Serial**	**Key Algorithm**	**Key Size**	**Sig. Algorithm**	**Not Before**	**Not After**	**SKI**	**SHA256 Fingerprint**
Public Certification Authority - G4	CN=Public Certification Authority - G4, O=Chunghwa Telecom Co., Ltd., C=TW	CN=ePKI Root Certification Authority - G4, O=Chunghwa Telecom Co., Ltd., C=TW	291c0c63c0172bb1259f5a425aaf24e3	rsaEncryption	4096 bits	sha256WithRSAEncryption	Nov 3 03:54:17 2022 GMT	Nov 3 15:59:59 2042 GMT	fe9a1c00b8c34bd0190d7592deca4fccccde7454	8FAF35AA59EBB971FB4FC6131DD9C2DA41C18421C86FDEC274606EC31EBE5436

中華電信

Other CA										
Common Name	**Subject**	**Issuer**	**Serial**	**Key Algorithm**	**Key Size**	**Sig. Algorithm**	**Not Before**	**Not After**	**SKI**	**SHA256 Fingerprint**
Public Certification Authority - G3	C=TW, O=Chunghwa Telecom Co., Ltd., CN=Public Certification Authority - G3	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G3	0088c1807ba0abb62e1f49a42a028be43e	rsaEncryption	2048 bits	sha256WithRSAEncryption	Apr 30 09:52:26 2019 GMT	Dec 31 15:59:59 2037 GMT	7b6b4b5754a5bb5d1a081ee986ec203b3951287c	B0F1F7C7DF837BDF88825A444444E4815DA7E0899728A07AE8767D5F65B50995

中華電信

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	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**
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

Secure Email (S/MIME) CA										
Common Name	**Subject**	**Issuer**	**Serial**	**Key Algorithm**	**Key Size**	**Sig. Algorithm**	**Not Before**	**Not After**	**SKI**	**SHA256 Fingerprint**
CHT SMIME CA - G1	C=TW, O=Chunghwa Telecom Co., Ltd., CN=CHT SMIME CA - G1	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G2	3878d76c8139e415898a37345e514650	rsaEncryption	4096 bits	sha256WithRSAEncryption	Jan 7 03:11:12 2021 GMT	Dec 29 16:00:00 2037 GMT	e985e072080d3922821a46a707ec514198476b4a	4AB2728FEC2114769461A2F5C2F51322497C7B923A0D8153E238F2AB073E3C2F
CHT SMIME CA - G2	CN=CHT SMIME CA - G2, O=hunghwa Telecom Co., Ltd., C=TW	CN=ePKI Root Certification Authority - G4, O=Chunghwa Telecom Co., Ltd., C=TW	09d94ead4f0a926b3cc6387c3582eab5	rsaEncryption	4096 bits	sha256WithRSAEncryption	Dec 21 02:29:51 2023 GMT	Dec 21 15:59:59 2038 GMT	4f7a5ab61048388c1211515058075e240912390c	15DC43B3BDA29DF4546008A4FC306DE811F3E78D804E1B989C2DE11D5336DA1A

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, WTCA

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