



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



19F.-5, No.171, Songde Rd., Sinyi District,
Taipei City 110, Taiwan, R.O.C.
Tel : +886 2 2346 6168
Fax : +886 2 2346 6068

INDEPENDENT ASSURANCE REPORT

To the management of Chunghwa Telecom Co., Ltd. (CHT):

We have been engaged, in a reasonable assurance engagement, to report on CHT management's assertion that for its Certification Authority (CA) operations at locations as enumerated in Appendix B, throughout the period 1 June 2025 to 31 May 2026 for its CAs as enumerated in Appendix A, CHT has:

- disclosed its 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



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

- 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 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



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

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 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



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

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 2025 to 31 May 2026, CHT management's assertion, as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities 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.

Other Matters

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

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

While the CHT's assertion notes all issues disclosed on Bugzilla through the audit period of this report, we have only noted those instances relevant to the CAs



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

enumerated in Appendix A and applicable to the WebTrust Principles and Criteria for Certification Authorities v2.2.2.

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

Use of the 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

August 10, 2026

DFK INTERNATIONAL



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



19F.-5, No.171, Songde Rd., Sinyi District,
Taipei City 110, Taiwan, R.O.C.
Tel : +886 2 2346 6168
Fax : +886 2 2346 6068

Appendix A-List of CAs in Scope(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	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
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	6237e01 b9aae4e 4df86229 bb44497 b01	rsaEncryption	4096 bits	sha256WithRSAEncryption	Apr 30 09:42:34 2019 GMT	Dec 31 15:59:59 2037 GMT	51ce2e18aca 1a4003549b a923bff095b bf3884ac	558FAB7F4B5DFF16 B68BA4E40D1D3E9 40EFA9B013350617 D6F377C1724D9D4 21



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	1890740 2b083ec 8bce199 4deafc0a 1d7	rsaEncryption	4096 bits	sha256WithRS AEncryption	Nov 17 08:31:41 2015 GMT	Dec 20 02:31:27 2034 GMT	1e0cf7b667f 2e19226094 5c055392e7 73f424aa2	B9C974DE139F6308 D74CCC423C3BC0B DED5E7AB4AD738B 304B50D429C42C3 D66
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	OU = ePKI Root Certification Authority O = Chunghwa	00edb8f4 6f99dd6a 9aa7623	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



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
	Telecom Co., Ltd. C = TW	Telecom Co., Ltd. C = TW	e3f2c11d 05c							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	sha256WithRS AEncryption	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 - 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
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

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	sha256WithRS AEncryption	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

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	291c0c63 c0172bb 1259f5a4 25aaf24e 3	rsaEncryption	4096 bits	sha256WithRS AEncryption	Nov 3 03:54:17 2022 GMT	Nov 3 15:59:59 2042 GMT	fe9a1c00b8c 34bd0190d7 592deca4fcc ccde7454	8FAF35AA59EBB97 1FB4FC6131DD9C2 DA41C18421C86FD EC274606EC31EBE5 436



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.,	C=TW, O=Chunghwa Telecom Co., Ltd.,	0088c18 07ba0ab	rsaEncryption	2048 bits	sha256WithRS AEncryption	Apr 30 09:52:26 2019 GMT	Dec 31 15:59:59 2037 GMT	7b6b4b5754 a5bb5d1a08 1ee986ec20 3b3951287c	B0F1F7C7DF837BD F88825A444444E48 15DA7E0899728A0 7AE8767D5F65B50 995
	CN=Public	CN=ePKI Root	b62e1f49							
	Certification	Certification	a42a028							
	Authority - G3	Authority - G3	be43e							



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



19F.-5, No.171, Songde Rd., Sinyi District,
Taipei City 110, Taiwan, R.O.C.
Tel : +886 2 2346 6168
Fax : +886 2 2346 6068

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

CAs Within the Audit Scope										
Common Name	Subject	Issuer	Serial	Key Algorithm	Key Size	Sig. Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
ePKI Root Certification Authority	C=TW, O=Chunghwa Telecom Co., Ltd., OU=ePKI Root Certification Authority	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G2	00cae1f7 3efcac5b b19c88c1 c72f6f7b 2f	rsaEncryption	4096 bits	sha256WithRSAEncryption	Nov 17 08:31:41 2015 GMT	Dec 20 02:31:27 2034 GMT	1e0cf7b667f 2e19226094 5c055392e7 73f424aa2	D108C34A58C0E4A 616449F8C4831802 3A229C86CD3DDD5 D5FE6041A401C16 A14
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	sha1WithRSAEncryption	May 16 10:13:55 2007 GMT	May 16 10:13:55 2027 GMT	71b35031a0 1b5b7bb2a6 597cfd108c3 cad3a3d7a	464B0EC0A602F019 3DB5F33911885A3 A61921AD16D2664 E25BEFAB10CFA6ED 25
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	sha1WithRSAEncryption	May 16 10:13:55 2007 GMT	May 16 10:13:55 2027 GMT	71b35031a0 1b5b7bb2a6 597cfd108c3 cad3a3d7a	4BD16F4955F3F3C9 C8EA48EF9995324D A5121724F89915D 5F2C91EB0BAEF233 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

CAs Within the Audit Sope										
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		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

CA out of the Audit Sope										
Common Name	Subject	Issuer	Serial	Key Algorithm	Key Size	Sig. Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint



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

政府伺服器數位憑證管理中心 - G1	CN = 政府伺服器數位憑證管理中心 - G1 O = 行政院 C = TW	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G2	00996d5f e9ade16c dc8ecdbf edb14a3 295	rsaEncryption	4096 bits	sha256WithRSAEncryption	Jul 19 06:46:45 2019 GMT	Aug 19 06:46:45 2031 GMT	d6eb2d9d61f e2bbb70882 eb807b159b 0f483226a	9D1CDA1B9EF395A FCE7DE0FE74DE6D 9FF5E0D2A4378911 6C00C6BA5BF44B9 823
--------------------	--	---	--	---------------	-----------	-------------------------	--------------------------------	--------------------------------	--	--



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



19F.-5, No.171, Songde Rd., Sinyi District,
Taipei City 110, Taiwan, R.O.C.
Tel : +886 2 2346 6168
Fax : +886 2 2346 6068

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

CP/CPS In-Scope

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

Locations In-Scope

CA Locations
Taipei, Taiwan
Taichung, Taiwan

MANAGEMENT'S ASSERTION OF CHUNGHWA TELECOM

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

- Subscriber Key Generation Services
- Subscriber Registration
- 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 locations as enumerated in Appendix B, throughout the period 1 June 2025 to 31 May 2026, 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

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.

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

Bug ID	Description	Date Opened	Date Closed
<u>2005567</u>	Chunghwa Telecom: CA Certificates Published in PEM format	2025-12-12	2026-02-03
<u>2005762</u>	Chunghwa Telecom: Failure to respond to CPR within 24 hours	2025-12-12	2026-02-05
<u>2008260</u>	Chunghwa Telecom: Delayed audit disclosure for GTLSCA	2026-01-01	2026-02-20
<u>2008782</u>	Chunghwa Telecom: Findings in 2025 WebTrust Audit - GTLSCA Audit Incident Report #1 - mass certificate revocation plan	2026-01-07	2026-02-18
<u>2008788</u>	Chunghwa Telecom: Findings in 2025 WebTrust Audit - GTLSCA Audit Incident Report #2 - Domain validation records without the TLS BR version	2026-01-07	2026-02-11
<u>2008799</u>	Chunghwa Telecom: Findings in 2025 WebTrust Audit - GTLSCA Audit Incident Report #3 - Missing vulnerability scan	2026-01-07	2026-02-20

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

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

Signature: Quen-Zong Wu

Title: Vice President

August 10, 2026

Appendix A-List of CAs in Scope(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	15c8bd65475c afb897005ee406d2bc9d	rsaEncryption	4096 bits	sha1WithRSAEncryption	Dec 20 02:31:27 2004 GMT	Dec 20 02:31:27 2034 GMT	1e0cf7b667f2e192260945c055392e773f424aa2	C0A6F4DC63A24BFDCF54EF2A6A082A0A72DE35803E2FF5FF527AE5D87206DFD5
ePKI Root Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G2	00d6962ec10a159312af8f63bcd44c95b	rsaEncryption	4096 bits	sha256WithRSAEncryption	Nov 17 08:23:42 2015 GMT	Dec 31 15:59:59 2037 GMT	725bbaaa7238ee259024b59422fa0988ca8b0afb	1E51942B84FD467BF77D1C89DA241C04254DC8F3EF4C22451FE7A89978BD4CD4F

Root CAs										
Common Name	Subject	Issuer	Serial	Key Algorithm	Key Size	Sig. Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
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	6237e01b9a ae4e4df86229bb44 497b01	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 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	2dddace629794a143e8b0cd766a5e60	rsaEncryption	4096 bits	sha256WithRSAEncryption	Feb 22 09:46:04 2019 GMT	Dec 31 15:59:59 2037 GMT	f27717fa5ea8fef63d71d568bac9460c38d8afb0	F015CE3CC239BFEF064BE9F1D2C417E1A0264A0A94BE1F0C8D121864EB6949CC

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

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

OV TLS Issuing CA										
Common Name	Subject	Issuer	Serial	Key Algorithm	Key Size	Sig. Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
Public Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., OU=Public Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., OU=ePKI Root Certification Authority	00c423d22191868fac4ee2fce4a011d1a7	rsaEncryption	2048 bits	sha256WithRSAEncryption	Dec 11 08:51:59 2014 GMT	Dec 11 08:51:59 2034 GMT	cb837d6515afa9c9f3a8a9f4647c795205744061	609930EB807AD420AFDA2A8AA61B67483039168CD766E09942A48BFE7F3BDC10
HiPKI OV TLS CA - G1	CN=HiPKI OV TLS CA - G1, O=Chunghwa Telecom Co., Ltd., C=TW	CN=HiPKI Root CA - G1, O=Chunghwa Telecom Co., Ltd., C=TW	2baba2d6e680cca594e04809af065d42	rsaEncryption	4096 bits	sha256WithRSAEncryption	May 18 02:51:28 2023 GMT	Dec 31 15:59:59 2037 GMT	358fc22e88de3313db0e2163ce542eb6824ca583	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	00b21437d0d67c63874844f8461c5f4b54	rsaEncryption	4096 bits	sha256WithRSAEncryption	Oct 18 02:50:29 2019 GMT	Dec 29 16:00:00 2037 GMT	d696a2d5966e2d3e40b1a3b26d88777bf6d6f4ca	DA31293D659781C69E0085C732A2811DB50E5CC576909149B80A98A9B0F93FD9

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	fe9a1c00b8c34bd0190d7592deca4fcccd7454	8FAF35AA59E BB971FB4FC6 131DD9C2DA 41C18421C86 FDEC274606E C31EBE5436

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

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

CAs Within the Audit Scope										
Common Name	Subject	Issuer	Serial	Key Algorithm	Key Size	Sig. Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
ePKI Root Certification Authority	C=TW, O=Chunghwa Telecom Co., Ltd., OU=ePKI Root Certification Authority	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G2	00cae1f73efcac5bb19c88c1c72f6f7b2f	rsaEncryption	4096 bits	sha256WithRSAEncryption	Nov 17 08:31:41 2015 GMT	Dec 20 02:31:27 2034 GMT	1e0cf7b667f2e192260945c055392e773f424aa2	D108C34A58C0E4A616449F8C48318023A229C86CD3DD5D5FE6041A401C16A14
Public Certification Authority	C=TW, O=Chunghwa Telecom Co., Ltd., OU=Public Certification Authority	C=TW, O=Chunghwa Telecom Co., Ltd., OU=ePKI Root Certification Authority	00c953feeb895e91884abb22a68a42a7d	rsaEncryption	2048 bits	sha1WithRSAEncryption	May 16 10:13:55 2007 GMT	May 16 10:13:55 2027 GMT	71b35031a01b5b7bb2a6597cfd108c3cad3a3d7a	464B0EC0A602F0193DB5F33911885A3A61921AD16D2664E25BEFAB10CFA6ED25

CAs Within the Audit Scope										
Common Name	Subject	Issuer	Serial	Key Algorithm	Key Size	Sig. Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
Public Certification Authority	C=TW, O=Chunghwa Telecom Co., Ltd., OU=Public Certification Authority	C=TW, O=Chunghwa Telecom Co., Ltd., OU=ePKI Root Certification Authority	00973c c94d44 cfe9a2 e14f52 e9a59 4a15a	rsaEncryption	2048 bits	sha1WithRSAEncryption	May 16 10:13:55 2007 GMT	May 16 10:13:55 2027 GMT	71b35031 a01b5b7b b2a6597c fd108c3c ad3a3d7a	4BD16F4955F 3F3C9C8EA48 EF9995324DA 5121724F8991 5D5F2C91EB0 BAEF2337
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	3878d 76c813 9e415 898a3 7345e 51465 0	rsaEncryption		sha256WithRSAEncryption	Jan 7 03:11:12 2021 GMT	Dec 29 16:00:00 2037 GMT	e985e072 080d3922 821a46a7 07ec5141 98476b4a	4AB2728FEC2 114769461A2F 5C2F5132249 7C7B923A0D8 153E238F2AB 073E3C2F
CHT SMIME CA - G2	CN=CHT SMIME CA - G2, O=Chunghwa Telecom Co., Ltd., C=TW	CN=ePKI Root Certification Authority - G4, O=Chunghwa Telecom Co., Ltd., C=TW	09d94 ead4f0 a926b 3cc638 7c3582 eab5	rsaEncryption	4096 bits	sha256WithRSAEncryption	Dec 21 02:29:51 2023 GMT	Dec 21 15:59:59 2038 GMT	4f7a5ab6 1048388c 12115150 58075e24 0912390c	15DC43B3BD A29DF454600 8A4FC306DE8 11F3E78D804 E1B989C2DE1 1D5336DA1A

CA out of the Audit Sope										
Common Name	Subject	Issuer	Serial	Key Algorithm	Key Size	Sig. Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
政府伺服器數位憑證管理中心 - G1	CN = 政府伺服器數位憑證管理中心 - G1 O = 行政院 C = TW	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G2	00996 d5fe9a de16cd c8ecdb fedb14 a3295	rsaEncryption	4096 bits	sha256WithRSAEncryption	Jul 19 06:46:45 2019 GMT	Aug 19 06:46:45 2031 GMT	d6eb2d9d 61fe2bbb 70882eb8 07b159b0 f483226a	9D1CDA1B9E F395AFCE7D E0FE74DE6D9 FF5E0D2A437 89116C00C6B A5BF44B9823

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

CP/CPS In-Scope

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

Locations In-Scope

CA Locations
Taipei, Taiwan
Taichung, Taiwan