



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



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

## INDEPENDENT ASSURANCE REPORT

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

We have been engaged, in a reasonable assurance engagement, to report on CHT management's assertion that for its Certification Authority (CA) operations at Taipei and Taichung, Taiwan, throughout the period 1 June 2024 to 31 May 2025 for its CAs as enumerated in Appendix A, for Network Security Requirements. CHT has:

- 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 – Network Security v1.7.](#)

### **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 – Network Security v1.7.

### **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



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

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 network and certificate system security to meet the requirements set forth by the CA/Browser Forum;
- (2) testing and evaluating the operating effectiveness of the controls; and
- (3) 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 2024 to 31 May 2025, CHT management's assertion, as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities – Network Security v1.7.

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 – Network Security v1.7, nor the suitability of any of CHT's services for any customer's intended purpose.

## Other Matters

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

Matter Topic		Matter Description
1	Delayed Annual Audit Report	CHT disclosed in Mozilla bug <a href="#">#1917224</a> that CHT did not upload audit reports to CCADB within 3 months after the end date of the annual audit period.

While the CHT's assertion notes all issues disclosed on Bugzilla through the audit period of this report, we have noted only those instances relevant to the CAs enumerated in Attachment A or applicable to the WebTrust Principles and Criteria for Certification Authorities – Network Security v1.7.

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



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

## Use of the WebTrust seal

CHT's use of the WebTrust for Certification Authorities –Network 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

August 8, 2025

DFK INTERNATIONAL



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



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

## Appendix A-List of CAs in Scope(Network Security)

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	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	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
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	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	00f670f9 5988f452 058e31e 168863ef a7a	rsaEncryption	4096 bits	sha256WithRSAEncryption	Nov 3 03:43:14 2022 GMT	Nov 3 15:59:59 2047 GMT	8dcf0a7c6f2 19db653aa4 6697cda3f75 6454a098	19A2FA09332C6D8 EAC1393D5F30371 DD8B4DD687B0E1E 50A6B48AE762CAB A2B5
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	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	sha256WithRS AEncryption	Nov 17 08:31:41 2015 GMT	Dec 20 02:31:27 2034 GMT	1e0cf7b667f 2e19226094 5c055392e7 73f424aa2	D108C34A58C0E4A 616449F8C4831802 3A229C86CD3DDD5 D5FE6041A401C16 A14
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	C=TW, O=Chunghwa Telecom Co., Ltd., OU=ePKI Root	00afcd8d 642c62d 645067d	rsaEncryption	4096 bits	sha256WithRS AEncryption	Nov 17 08:51:35 2015 GMT	Dec 20 02:31:27 2034 GMT	725bbaaa72 38ee259024	18467C4E64D586C 844A44466DE5BA7 A6D5969C7A92859



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	c857fda8 f15d						b59422fa098 8ca8b0afb	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
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	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	464B0ECO0A602F019 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	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	597419b53						9f4647c795205744061	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

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	7239e9d 901bcd1 96e3658 d9277db 3470	rsaEncryption	4096 bits	sha256WithRSAEncryption	Jan 7 03:11:12 2021 GMT	Dec 29 16:00:00 2037 GMT	e985e07208 0d3922821a 46a707ec51 4198476b4a	5EB6CC7D03C349B 2DCC5BDD7B10141 FC7AB8AE1844944F 6950BE741D3D731 C95
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	3878d76 c8139e41 5898a37 345e514 650	rsaEncryption	4096 bits	sha256WithRSAEncryption	Jan 7 03:11:12 2021 GMT	Dec 29 16:00:00 2037 GMT	e985e07208 0d3922821a 46a707ec51 4198476b4a	4AB2728FEC211476 9461A2F5C2F51322 497C7B923A0D815 3E238F2AB073E3C2 F
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	sha256WithRSAEncryption	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

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., CN=Public Certification Authority - G3	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G3	0088c18 07ba0ab b62e1f49 a42a028 be43e	rsaEncryption	2048 bits	sha256WithRS AEncryption	Apr 30 09:52:26 2019 GMT	Dec 31 15:59:59 2037 GMT	7b6b4b5754 a5bb5d1a08 1ee986ec20 3b3951287c	BOF1F7C7DF837BD F88825A444444E48 15DA7E0899728A0 7AE8767D5F65B50 995



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



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

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

N/A

## MANAGEMENT'S ASSERTION OF CHUNGHWA TELECOM

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

The management of CHT is responsible for establishing and maintaining effective controls over its CA operations, including its network and certificate security system 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 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 2024 to 31 May 2025, CHT has:

- 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 – Network Security v1.7](#).

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

Bug ID	Description	Date Opened	Date Closed
<a href="#">#1904038</a>	"Test Website - Valid" URL disclosed to CCADB is expired	2024-06-21	2025-04-18

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

Signature: Quen-Zong Wu

Title: Vice President

August 8, 2025

**Appendix A-List of CAs in Scope(Network Security)**

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	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	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
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	558FAB7F4B5DFF16 B68BA4E40D1D3E9 40EFA9B013350617 D6F377C1724D9D4 21
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	19A2FA09332C6D8 EAC1393D5F30371 DD8B4DD687B0E1E 50A6B48AE762CAB A2B5

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	2dddacce 629794a 143e8b0 cd766a5e 60	rsaEncryption	4096 bits	sha256WithRS AEncryption	Feb 22 09:46:04 2019 GMT	Dec 31 15:59:59 2037 GMT	f27717fa5ea 8fef63d71d5 68bac9460c3 8d8afb0	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	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	00cae1f73efcac5b b19c88c1 c72f6f7b 2f	rsaEncryption	4096 bits	sha256WithRSAEncryption	Nov 17 08:31:41 2015 GMT	Dec 20 02:31:27 2034 GMT	1e0cf7b667f2e192260945c055392e773f424aa2	D108C34A58C0E4A616449F8C48318023A229C86CD3DD5D5FE6041A401C16A14
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

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
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	00c953fee895e91884ab22a68a42a7d	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	DAE3434F696FC9F0F652E1B2A6F69B5E9273D09F43BD3BD4717D6141F8CD2C2

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

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	7239e9d 901bcd1 96e3658 d9277db 3470	rsaEncryption	4096 bits	sha256WithRSAEncryption	Jan 7 03:11:12 2021 GMT	Dec 29 16:00:00 2037 GMT	e985e07208 0d3922821a 46a707ec51 4198476b4a	5EB6CC7D03C349B 2DCC5BDD7B10141 FC7AB8AE1844944F 6950BE741D3D731 C95
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	3878d76 c8139e41 5898a37 345e514 650	rsaEncryption	4096 bits	sha256WithRSAEncryption	Jan 7 03:11:12 2021 GMT	Dec 29 16:00:00 2037 GMT	e985e07208 0d3922821a 46a707ec51 4198476b4a	4AB2728FEC211476 9461A2F5C2F51322 497C7B923A0D815 3E238F2AB073E3C2 F
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	sha256WithRSAEncryption	Dec 21 02:29:51 2023 GMT	Dec 21 15:59:59 2038 GMT	4f7a5ab6104 8388c12115 15058075e2 40912390c	15DC43B3BDA29DF 4546008A4FC306D E811F3E78D804E1B 989C2DE11D5336D A1A

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

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	0088c18 07ba0ab b62e1f49 a42a028 be43e	rsaEncryption	2048 bits	sha256WithRS AEncryption	Apr 30 09:52:26 2019 GMT	Dec 31 15:59:59 2037 GMT	7b6b4b5754 a5bb5d1a08 1ee986ec20 3b3951287c	BOF1F7C7DF837BD F88825A444444E48 15DA7E0899728A0 7AE8767D5F65B50 995



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

N/A



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

N/A