



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 for S/MIME Baseline Requirements, CHT has:

- disclosed its S/MIME certificate lifecycle management business practices in the applicable versions of its CHT Certification Practice Statement ("CPS") and CHT Certificate Policy ("CP") as enumerated in Appendix B

including its commitment to provide S/MIME certificates in conformity with the CA/Browser Forum Requirements on the CHT website, and provided such services in accordance with its disclosed practices

- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and S/MIME certificates it manages is established and protected throughout their lifecycles; and
  - S/MIME subscriber information is properly authenticated (for the registration activities performed by CHT)
- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorized individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity

in accordance with the [WebTrust Principles and Criteria for Certification Authorities – S/MIME Certificates v1.0.](#)



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



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

## **Certification authority's responsibilities**

CHT's management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities – S/MIME Certificates v1.0.

## **Our independence and quality control**

We have complied with the independence and other ethical requirements of the Code of Ethics for Professional Accountants issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

The firm applies International Standard on Quality Management (ISQM) 1, Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

## **Auditor's responsibilities**

Our responsibility is to express an opinion on management's assertion based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, Assurance Engagements Other than Audits or Reviews of Historical Financial Information, issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's assertion is fairly stated, and, accordingly, included:

- (1) obtaining an understanding of CHT's 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;



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

- (2) obtaining an understanding of CHT's S/MIME certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of S/MIME certificates;
- (3) selectively testing transactions executed in accordance with disclosed key and certificate lifecycle management business practices;
- (4) testing and evaluating the operating effectiveness of the controls; and
- (5) performing such other procedures as we considered necessary in the circumstances.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

### **Relative effectiveness of controls**

The relative effectiveness and significance of specific controls at CHT and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

### **Inherent limitations**

Because of the nature and inherent limitations of controls, CHT's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

### **Opinion**

In our opinion, throughout the period 1 June 2023 to 31 May 2024, CHT management's assertion, as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities – S/MIME Certificates v1.0.

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



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

Authorities – S/MIME Certificates v1.0, 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 – S/MIME Certificates 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( S/MIME)

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	sha1WithRSAE ncryption	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	sha256WithRS AEncryption	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 - 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	sha256WithRS AEncryption	Nov 3 03:43:14 2022 GMT	Nov 3 15:59:59 2047 GMT	8dcf0a7c6f2 19db653aa4 6697cda3f75 6454a098	19A2FA09332C6D8 EAC1393D5F30371 DD8B4DD687B0E1E 50A6B48AE762CAB A2B5



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



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

Cross-Signed CA Certificates										
Common Name	Subject	Issuer	Serial	Key Algorithm	Key Size	Sig. Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
ePKI Root Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., OU=ePKI Root Certification Authority	3beee09 18e8886 ad460fe8 ae910c9c ba	rsaEncryption	4096 bits	sha256WithRS AEncryption	Nov 17 08:51:35 2015 GMT	Dec 20 02:31:27 2034 GMT	725bbaaa72 38ee259024 b59422fa098 8ca8b0afb	64717250AF8B028 DD8E5C0BAE4C914 2C8B103532612BC 487085FD3C319F9C 067
ePKI Root Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., OU=ePKI Root Certification Authority	00afcd8d 642c62d 645067d c857fda8 f15d	rsaEncryption	4096 bits	sha256WithRS AEncryption	Nov 17 08:51:35 2015 GMT	Dec 20 02:31:27 2034 GMT	725bbaaa72 38ee259024 b59422fa098 8ca8b0afb	18467C4E64D586C 844A44466DE5BA7 A6D5969C7A92859 A511C5FDAD75B03 CDCE
ePKI Root Certification Authority - G2	CN = ePKI Root Certification Authority - G2 O = Chunghwa Telecom Co., Ltd. C = TW	OU = ePKI Root Certification Authority O = Chunghwa Telecom Co., Ltd. C = TW	00edb8f4 6f99dd6a 9aa7623 e3f2c11d 05c	rsaEncryption	4096 bits	sha256WithRS AEncryption	Nov 17 08:51:35 2015 GMT	Dec 20 02:31:27 2034 GMT	725bbaaa72 38ee259024 b59422fa098 8ca8b0afb	72D716F7BB6BD10 5704F42B95249235 10DCB85B2D870C0 E9ADA5AEB9C9690 51A



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



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

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

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

Cross-Signed CA Certificates										
Common Name	Subject	Issuer	Serial	Key Algorithm	Key Size	Sig. Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
ePKI Root Certification Authority - G2	CN = ePKI Root Certification Authority - G2 O = Chunghwa Telecom Co., Ltd. C = TW	OU = ePKI Root Certification Authority O = Chunghwa Telecom Co., Ltd. C = TW	00edb8f4 6f99dd6a 9aa7623 e3f2c11d 05c	rsaEncryption	4096 bits	sha256WithRS AEncryption	Nov 17 08:51:35 2015 GMT	Dec 20 02:31:27 2034 GMT	725bbaaa72 38ee259024 b59422fa098 8ca8b0afb	72D716F7BB6BD10 5704F42B95249235 10DCB85B2D870C0 E9ADA5AEB9C9690 51A





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



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

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



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, S/MIME

Document Name	Version	Effective Date
<a href="#">ePKI CP</a>	V2.1	August 29, 2023
<a href="#">ePKI CP</a>	V2.05	December 7, 2022
<a href="#">CHTCA CPS</a>	V1.07	May 06, 2024
<a href="#">CHTCA CPS</a>	V1.05	August 29, 2023
<a href="#">CHTCA CPS</a>	V1.0	April 6, 2023

## MANAGEMENT'S ASSERTION OF CHUNGHWA TELECOM

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

The management of CHT is responsible for establishing and maintaining effective controls over its S/MIME CA operations, including its S/MIME CA business practices disclosure on its website, S/MIME key lifecycle management controls, and S/MIME 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 S/MIME CA services at Taipei and Taichung, Taiwan, throughout the period 1 June 2023 to 31 May 2024, CHT has:

- disclosed its S/MIME certificate life cycle management business practices in the applicable versions of its CHT Certification Practice Statement ("CPS") and CHT Certificate Policy ("CP") as enumerated in Appendix B.

including its commitment to provide S/MIME certificates in conformity with the CA/Browser Forum Requirements on the CHT website, and provided such services in accordance with its disclosed practices

- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and S/MIME certificates it manages is established and protected throughout their lifecycles; and
  - S/MIME certificate subscriber information is properly authenticated (for the registration activities performed by CHT)
- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorised individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorised and performed to maintain CA systems integrity
- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

in accordance with the [WebTrust Principles and Criteria for Certification Authorities – S/MIME Certificates v1.0.](#)

Signature: Quen-Zong Wu

Title: Vice President

October 22, 2024

## Appendix A-List of CAs in Scope( S/MIME)

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	C0A6F4DC63A24BF DCF54EF2A6A082A 0A72DE35803E2FF5 FF527AE5D87206D FD5
ePKI Root Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G2	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 - 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

Cross-Signed CA Certificates										
Common Name	Subject	Issuer	Serial	Key Algorithm	Key Size	Sig. Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
ePKI Root Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., OU=ePKI Root Certification Authority	3beee09 18e8886 ad460fe8 ae910c9c ba	rsaEncryption	4096 bits	sha256WithRS AEncryption	Nov 17 08:51:35 2015 GMT	Dec 20 02:31:27 2034 GMT	725bbaaa72 38ee259024 b59422fa098 8ca8b0afb	64717250AF8B028 DD8E5C0BAE4C914 2C8B103532612BC 487085FD3C319F9C 067
ePKI Root Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., OU=ePKI Root Certification Authority	00afcd8d 642c62d 645067d c857fda8 f15d	rsaEncryption	4096 bits	sha256WithRS AEncryption	Nov 17 08:51:35 2015 GMT	Dec 20 02:31:27 2034 GMT	725bbaaa72 38ee259024 b59422fa098 8ca8b0afb	18467C4E64D586C 844A44466DE5BA7 A6D5969C7A92859 A511C5FDAD75B03 CDCE
ePKI Root Certification Authority - G2	CN = ePKI Root Certification Authority - G2 O = Chunghwa Telecom Co., Ltd. C = TW	OU = ePKI Root Certification Authority O = Chunghwa Telecom Co., Ltd. C = TW	00edb8f4 6f99dd6a 9aa7623 e3f2c11d 05c	rsaEncryption	4096 bits	sha256WithRS AEncryption	Nov 17 08:51:35 2015 GMT	Dec 20 02:31:27 2034 GMT	725bbaaa72 38ee259024 b59422fa098 8ca8b0afb	72D716F7BB6BD10 5704F42B95249235 10DCB85B2D870C0 E9ADA5AEB9C9690 51A

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=Chunghwa 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.1-List of CA Certificates issued During the Audit Period

Cross-Signed CA Certificates										
Common Name	Subject	Issuer	Serial	Key Algorithm	Key Size	Sig. Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint
ePKI Root Certification Authority - G2	CN = ePKI Root Certification Authority - G2 O = Chunghwa Telecom Co., Ltd. C = TW	OU = ePKI Root Certification Authority O = Chunghwa Telecom Co., Ltd. C = TW	00edb8f4 6f99dd6a 9aa7623 e3f2c11d 05c	rsaEncryption	4096 bits	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

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

## Appendix B- Certificate Policy and Certification Practice Statement Versions in Scope, S/MIME

Document Name	Version	Effective Date
<a href="#">ePKI CP</a>	V2.1	August 29, 2023
<a href="#">ePKI CP</a>	V2.05	December 7, 2022
<a href="#">CHTCA CPS</a>	V1.07	May 06, 2024
<a href="#">CHTCA CPS</a>	V1.05	August 29, 2023
<a href="#">CHTCA CPS</a>	V1.0	April 6, 2023