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 (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 2019 to 31 May 2020 for its CAs as enumerated in Appendix A, CHT has:

- disclosed its SSL certificate life cycle management business practices in in the applicable versions of its CHT Certification Practice Statement ("CPS") and CHT Certificate Policy ("CP") as enumerated in Appendix B including its commitment to provide SSL and non-SSL certificates in conformity with the CA/Browser Forum Requirements on the CHT website, and provided such services in accordance with its disclosed practices

- maintained effective controls to provide reasonable assurance that:
    - the integrity of keys and SSL certificates it manages is established and protected throughout their lifecycles; and
    - SSL certificate subscriber information is properly authenticated

- maintained effective controls to provide reasonable assurance that:
    - logical and physical access to CA systems and data is restricted to authorized individuals;
    - the continuity of key and certificate management operations is maintained; and
    - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity

- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.4.1.

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

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

Certification authority's responsibilities

CHT's management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.4.1.

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 Control 1, and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Auditor's responsibilities

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

(1) obtaining an understanding of CHT's SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of SSL certificates, and obtaining an understanding of CHT's network and certificate system security to meet the requirements set forth by the CA/Browser Forum;
(2) selectively testing transactions executed in accordance with disclosed SSL certificate lifecycle management business practices;
(3) testing and evaluating the operating effectiveness of the controls; and

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

(4) performing such other procedures as we considered necessary in the circumstances.

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

Relative effectiveness of controls

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

Inherent limitations

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

Opinion

In our opinion, throughout the period 1 June 2019 to 31 May 2020, CHT management's assertion, as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.4.1.

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

(1). CHT disclosed publicly on the Mozilla's Bugzilla Platform the incident (Bug 1532436). In this incident, 2 certificates with unregistered FQDN were mis-issued. The details of the incident and the remediation taken by CHT were illustrated in Appendix C.

(2). A particular risk pertaining to the segregation between the Public Certification Authority - G2 and the Public Certification Authority - G3 was identified during the audit process. No certificate was found to be mis-issued due to this

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

matter. The nature of this risk and additional controls were illustrated in Appendix D.

We have noted any instance possible non-compliance that are relevant to the CAs enumerated in Appendix A. CHT's assertion noted all instances possible non-compliance, addressed by CHT, during the engagement period, regardless of the particular CAs enumerated in Appendix A.

This report does not include any representation as to the quality of CHT's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.4.1, nor the suitability of any of CHT's services for any customer's intended purpose.

Use of the WebTrust seal

CHT's use of the WebTrust for Certification Authorities – SSL Baseline with Network 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 24, 2020

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

Root CAs										
Common Name	**Subject**	**Issuer**	**Serial**	**Key Algorithm**	**Key Size**	**Sig. Algorithm**	**Not Before**	**Not After**	**SKI**	**SHA256 Fingerprint**
ePKI Root Certification Authority	OU = ePKI Root Certification Authority O = Chunghwa Telecom Co., Ltd. C = TW	OU = ePKI Root Certification Authority O = Chunghwa Telecom Co., Ltd. C = TW	15c8bd65475cafb897005ee406d2bc9d	rsaEncryption	4096 bits	sha1WithRSAEncryption	Dec 20 02:31:27 2004 GMT	Dec 20 02:31:27 2034 GMT	1e0cf7b667f2e192260945c055392e773f424aa2	c0a6f4dc63a24bfdcf54ef2a6a082a0a72de35803e2ff5ff527ae5d87206dfd5
ePKI Root Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G2	00d6962ec10a159312af8f63bcd444c95b	rsaEncryption	4096 bits	sha256WithRSAEncryption	Nov 17 08:23:42 2015 GMT	Dec 31 15:59:59 2037 GMT	725bbaaa7238ee259024b59422fa0988ca8b0afb	1e51942b84fd467bf77d1c89da241c04254dc8f3ef4c22451fe7a89978bdcd4f
ePKI Root Certification Authority - G3	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G3	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G3	6237e01b9aae4e4df86229bb44497b01	rsaEncryption	4096 bits	sha256WithRSAEncryption	Apr 30 09:42:34 2019 GMT	Dec 31 15:59:59 2037 GMT	51ce2e18aca1a4003549ba923bff095bbf3884ac	558fab7f4b5dff16b68ba4e40d1d3e940efa9b013350617d6f377c1724d9d421

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

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

Root CAs										
Common Name	**Subject**	**Issuer**	**Serial**	**Key Algorithm**	**Key Size**	**Sig. Algorithm**	**Not Before**	**Not After**	**SKI**	**SHA256 Fingerprint**
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

Cross-Signed CA Certificates										
Common Name	**Subject**	**Issuer**	**Serial**	**Key Algorithm**	**Key Size**	**Sig. Algorithm**	**Not Before**	**Not After**	**SKI**	**SHA256 Fingerprint**
ePKI Root Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., OU=ePKI Root Certification Authority	3beee0918e8886ad460fe8ae910c9cba	rsaEncryption	4096 bits	sha256WithRSAEncryption	Nov 17 08:51:35 2015 GMT	Dec 20 02:31:27 2034 GMT	725bbaaa7238ee259024b59422fa0988ca8b0afb	64717250af8b028dd8e5c0bae4c9142c8b103532612bc487085fd3c319f9c067
ePKI Root Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., OU=ePKI Root Certification Authority	00afcd8d642c62d645067dc857fda8f15d	rsaEncryption	4096 bits	sha256WithRSAEncryption	Nov 17 08:51:35 2015 GMT	Dec 20 02:31:27 2034 GMT	725bbaaa7238ee259024b59422fa0988ca8b0afb	18467c4e64d586c844a44466de5ba7a6d5969c7a92859a511c5fdad75b03cdce

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

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

Cross-Signed CA Certificates										
Common Name	**Subject**	**Issuer**	**Serial**	**Key Algorithm**	**Key Size**	**Sig. Algorithm**	**Not Before**	**Not After**	**SKI**	**SHA256 Fingerprint**
ePKI Root Certification Authority	C=TW, O=Chunghwa Telecom Co., Ltd., OU=ePKI Root Certification Authority	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G2	00cae1f73efcac5bb19c88c1c72f6f7b2f	rsaEncryption	4096 bits	sha256WithRSAEncryption	Nov 17 08:31:41 2015 GMT	Dec 20 02:31:27 2034 GMT	1e0cf7b667f2e192260945c055392e773f424aa2	d108c34a58c0e4a616449f8c48318023a229c86cd3ddd5d5fe6041a401c16a14
ePKI Root Certification Authority	C=TW, O=Chunghwa Telecom Co., Ltd., OU=ePKI Root Certification Authority	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G2	18907402b083ec8bce1994deafc0a1d7	rsaEncryption	4096 bits	sha256WithRSAEncryption	Nov 17 08:31:41 2015 GMT	Dec 20 02:31:27 2034 GMT	1e0cf7b667f2e192260945c055392e773f424aa2	b9c974de139f6308d74ccc423c3bc0bded5e7ab4ad738b304b50d429c42c3d66

OV SSL Issuing CAs										
Common Name	**Subject**	**Issuer**	**Serial**	**Key Algorithm**	**Key Size**	**Sig. Algorithm**	**Not Before**	**Not After**	**SKI**	**SHA256 Fingerprint**
Public Certification Authority	C=TW, O=Chunghwa Telecom Co., Ltd., OU=Public Certification Authority	C=TW, O=Chunghwa Telecom Co., Ltd., OU=ePKI Root Certification Authority	00c953feeeb895e91884abb22a68a42a7d	rsaEncryption	2048 bits	sha1WithRSAEncryption	May 16 10:13:55 2007 GMT	May 16 10:13:55 2027 GMT	71b35031a01b5b7bb2a6597cfd108c3cad3a3d7a	464b0ec0a602f0193db5f33911885a3a61921ad16d2664e25befab10cfa6ed25

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 SSL Issuing CAs										
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	00973cc94d44cfe9a2e14f52e9a594a15a	rsaEncryption	2048 bits	sha1WithRSAEncryption	May 16 10:13:55 2007 GMT	May 16 10:13:55 2027 GMT	71b35031a01b5b7bb2a6597cfd108c3cad3a3d7a	4bd16f4955f3f3c9c8ea48ef9995324da5121724f89915d5f2c91eb0baef2337
Public Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., OU=Public Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., OU=ePKI Root Certification Authority	00c423d22191868fac4ee2fce4a011d1a7	rsaEncryption	2048 bits	sha256WithRSAEncryption	Dec 11 08:51:59 2014 GMT	Dec 11 08:51:59 2034 GMT	cb837d6515afa9c9f3a8a9f4647c795205744061	609930eb807ad420afda2a8aa61b67483039168cd766e09942a48bfe7f3bdc10
Public Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., OU=Public Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., OU=ePKI Root Certification Authority	143596f2441a7167983ffc9597419b53	rsaEncryption	2048 bits	sha256WithRSAEncryption	Dec 11 08:51:59 2014 GMT	Dec 11 08:51:59 2034 GMT	cb837d6515afa9c9f3a8a9f4647c795205744061	dae3434f696fc9f0f652e1b2a6f69b5e9273d09f43bd3bdd4717d6141f8cd2c2
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

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

EV SSL Issuing CAs										
Common Name	**Subject**	**Issuer**	**Serial**	**Key Algorithm**	**Key Size**	**Sig. Algorithm**	**Not Before**	**Not After**	**SKI**	**SHA256 Fingerprint**
HiPKI EV TLS CA - G1	C=TW, O=Chunghwa Telecom Co., Ltd., CN=HiPKI EV TLS CA - G1	C=TW, O=Chunghwa Telecom Co., Ltd., CN=HiPKI Root CA - G1	3c43cdcddcf23b004f0ea073fc3ea389	rsaEncryption	4096 bits	sha256WithRSAEncryption	Feb 22 09:56:03 2019 GMT	Dec 31 15:59:59 2037 GMT	a90dea63aee38c0340e7ffdc3328e5238ecb109b	2a8e6a86e74d10edb2026c81693d64957a0f081c1631912ac95efdfcb5625657

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

Document Name	Version	Effective Date
ePKI CP	V1.8	November 18, 2019
ePKI CP	V1.75	August 12, 2019
ePKI CP	V1.7	April 30, 2019
eCA CPS	V1.7	April 22, 2020
eCA CPS	V1.67	November 18, 2019
eCA CPS	V1.65	August 30, 2019
eCA CPS	V1.6	April 30, 2019
PublicCA CPS	V2.0	April 22, 2020
PublicCA CPS	V1.9	April 30, 2019
HiPKI CP	V1.05	March 2, 2020
HiPKI CP	V1.0	February 22, 2019
HiPKI RCA CPS	V1.05	March 2, 2020
HiPKI RCA CPS	V1.0	February 22, 2019
EV TLS CA CPS	V1.05	March 2, 2020
EV TLS CA CPS	V1.0	February 22, 2019

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

Appedix C- Incidents and Remediation

Incident

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

Bugzilla Number: Bug 1532436

Opened Date: March 4, 2019

Status: Open

Certificates Issued By: Public Certification Authority - G2

Description:

A certificate with unregistered FQDN www.raotest.com.tw was mis-issued on November 12, 2018 11:53:02 (UTC) and revoked on 15 February 2019 1:59; a certificate with unregistered FQDN publicca.rao.com.tw was mis-issued on January 29, 2019 06:43:59 (UTC) and revoked immediately. These two certificates were issued by the same RAO because the RAO intended to take a screenshot of certificate application process for training material.

Remediation

(1). To implement a two-stage manual verification by different RAOs.

This control has been in place since February 26, 2019.

(2). To implement an automatic FQDN-checking function.

This automatic FQDN-checking function went live on March 15, 2019.

The tested scenarios were summarized as follows:

Scenario	Expected Outcome	Test Result	Deployment Date and Change Request Number
Query the FQDN with WHOIS and find the applied-for FQDN is unregistered.	Rejected	Satisfactory	2019-03-15 CR # 1080315
Query the FQDN with WHOIS and find the applied-for FQDN is unregistered.	Rejected	Satisfactory	2019-03-15 CR # 1080315

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

Scenario	Expected Outcome	Test Result	Deployment Date and Change Request Number
The RAO modifies the status of the application ticket and triggers the issuance function.			

The test result indicated the function was satisfied.

(3). To implement an automatic domain control validation function.

Test cases were developed according to the functionality and the BR validation requirements. The test result indicated the function was satisfied.

The tested scenarios, the corresponding BR validation requirements and the deployment date were summarized as follows:

Scenario	BR Validation Requirement	Expected Outcome	Test Result	Deployment Date and Change Request Number
Query the FQDN with WHOIS. The Registrar is HINET and the organization name of the FQDN matches with the full name on the SSL application form.	3.2.2.4.12	Passed	Satisfactory	2020-02-19 CR #1090219
Query the FQDN with WHOIS. The Registrar is HINET but the organization name of the FQDN does not match with the full name on the SSL application form.	3.2.2.4.12	Rejected	Satisfactory	2020-02-19 CR #1090219
Query the FQDN with WHOIS. The Registrar is not HINET; The organization name of the FQDN matches with the full name on the SSL application form; and The Contact email of the FQDN matches with the technical person's email	3.2.2.4.2	Passed	Satisfactory	2020-06-22 CR #1090622-2
Query the FQDN with WHOIS. The Registrar is not HINET;	3.2.2.4.2	Rejected	Satisfactory	2020-06-22 CR #1090622-2

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

Scenario	BR Validation Requirement	Expected Outcome	Test Result	Deployment Date and Change Request Number
The organization name of the FQDN matches with the full name on the SSL application form; and The Contact email of the FQDN does not match with the technical person's email				
Query the FQDN with WHOIS. The Registrar is not HINET. The organization name of the FQDN does not match with the full name on the SSL application form.	3.2.2.4.2	Rejected	Satisfactory	2020-06-22 CR #1090622-2
Send an email to the technical person's email address on the SSL application form with a file containing a random value. Ask the person to put the file under the .well-known/pki-validation/ directory of the FQDN. The random value is correct and not expired.	3.2.2.4.6	Passed	Satisfactory	2020-02-19 CR #1090219
Send an email to the technical person's email address on the SSL application form with a file containing a random value. Ask the person to put the file under the .well-known/pki-validation/ directory of the FQDN. The file is missing.	3.2.2.4.6	Rejected	Satisfactory	2020-02-19 CR #1090219
Send an email to the technical person's email address on the SSL application form with a file containing a random value. Ask the person to put the file under the .well-known/pki-validation/ directory of the FQDN. The random value is incorrect.	3.2.2.4.6	Rejected	Satisfactory	2020-02-19 CR #1090219

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

Scenario	BR Validation Requirement	Expected Outcome	Test Result	Deployment Date and Change Request Number
Send an email to the technical person's email address on the SSL application form with a file containing a random value. Ask the person to put the file under the .well-known/pki-validation/ directory of the FQDN. The random value is correct but expired.	3.2.2.4.6	Rejected	Satisfactory	2020-02-19 CR #1090219
Send an email to the technical person's email address on the SSL application form with a file containing a random value. Ask the person to put the file under the .well-known/pki-validation/ directory of the FQDN. The URL is redirected to different website (http return code:3xx) The file can be found. The random value is correct and not expired.	3.2.2.4.18	Passed	Satisfactory	2020-05-25 CR #1090525
Send an email to the technical person's email address on the SSL application form with a file containing a random value. Ask the person to put the file under the .well-known/pki-validation/ directory of the FQDN. The URL is redirected to different page of the same website (http return code:3xx) The file can be found. The random value is correct and not expired.	3.2.2.4.18	Passed	Satisfactory	2020-05-25 CR #1090525
Send an email to the technical person's email address on the SSL application form with a file containing a random value.	3.2.2.4.18	Rejected	Satisfactory	2020-05-25 CR #1090525

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

Scenario	BR Validation Requirement	Expected Outcome	Test Result	Deployment Date and Change Request Number
Ask the person to put the file under the .well-known/pki-validation/ directory of the FQDN. The URL is redirected to different website (http return code:3xx) The file can be found. The random value is incorrect.				
Send an email to the technical person's email address on the SSL application form with a file containing a random value. Ask the person to put the file under the .well-known/pki-validation/ directory of the FQDN. The URL is redirected to different website (http return code:3xx) The file can be found. The random value is expired.	3.2.2.4.18	Rejected	Satisfactory	2020-05-25 CR #1090525
Send an email to the technical person's email address on the SSL application form with a file containing a random value. Ask the person to put the file under the .well-known/pki-validation/ directory of the FQDN. The URL is redirected to different page of the same website (http return code:3xx) The file cannot be found.	3.2.2.4.18	Rejected	Satisfactory	2020-05-25 CR #1090525
Send an email to the technical person's email address on the SSL application form with a file containing a random value. Ask the person to put the file under the .well-known/pki-validation/ directory of the FQDN.	3.2.2.4.18	Rejected	Satisfactory	2020-05-25 CR #1090525

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

Scenario	BR Validation Requirement	Expected Outcome	Test Result	Deployment Date and Change Request Number
The URL is redirected to different page of the same website (http return code:3xx) The file can be found. The random value is incorrect .				
Send an email to the technical person's email address on the SSL application form with a file containing a random value. Ask the person to put the file under the .well-known/pki-validation/ directory of the FQDN. The URL is redirected to different page of the same website (http return code:3xx) The file can be found. The random value is expired.	3.2.2.4.18	Rejected	Satisfactory	2020-05-25 CR #1090525
Send an email to the technical person's email address on the SSL application form with a random value in the content. Ask the person to put the random value in the DNS TXT Record by the required format.	3.2.2.4.7	Passed	Satisfactory	2019-06-10 CR #1080610-2
Send an email to the technical person's email address on the SSL application form with a random value in the content. Ask the person to put the random value in the DNS TXT Record by the required format. The system periodically checks with the dig command and finds the value is incorrect.	3.2.2.4.7	Rejected	Satisfactory	2019-06-10 CR #1080610-2
Send an email to the technical person's email address on the SSL application form with a random value in the content.	3.2.2.4.7	Rejected	Satisfactory	2019-06-10 CR #1080610-2

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

Scenario	BR Validation Requirement	Expected Outcome	Test Result	Deployment Date and Change Request Number
Ask the person to put the random value in the DNS TXT Record by the required format. The system periodically checks with the dig command and finds the value is correct but expired.				
Query the FQDN with WHOIS. Send an email to the registrant email with confirming link with the random value. The email recipient clicks the link and is directed to the authorization link. The email recipient clicks the authorization link.	3.2.2.4.2	Passed	Satisfactory	2020-06-22 CR #1090622-2
Query the FQDN with WHOIS. Send an email to the registrant email with confirming link of the random value. The email recipient modifies the link and clicks the link.	3.2.2.4.2	Rejected	Satisfactory	2020-06-22 CR #1090622-2
Query the FQDN with WHOIS. Send an email to the registrant email with confirming link of the random value. The email recipient clicks the link after 30 days.	3.2.2.4.2	Rejected	Satisfactory	2020-06-22 CR #1090622-2
Send an email to the postmaster, webmaster, hostmaster of the FQDN with confirming link of the random value. The email recipient clicks the link and is directed to the conformation webpage	3.2.2.4.4	Passed	Satisfactory	2020-02-19 CR #1090219
Send an email to the postmaster, webmaster, hostmaster of the FQDN with confirming link of the random value. The email recipient modifies the link and clicks the link.	3.2.2.4.4	Rejected	Satisfactory	2020-02-19 CR #1090219
Send an email to the postmaster, webmaster, hostmaster of the	3.2.2.4.4	Rejected	Satisfactory	2020-02-19 CR #1090219

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

Scenario	BR Validation Requirement	Expected Outcome	Test Result	Deployment Date and Change Request Number
FQDN with confirming link of the random value. The email recipient clicks the link after 30 days.				
Send an email to the TXT contact email and the CAA contact email in the DNS. The email recipient clicks the link and is directed to the confirmation webpage.	3.2.2.4.13 3.2.2.4.14	Passed	Satisfactory	2020-06-11 CR #1090611
Send an email to the TXT contact email and the CAA contact email in the DNS. The email recipient modifies the link and clicks the link.	3.2.2.4.13 3.2.2.4.14	Rejected	Satisfactory	2020-06-11 CR #1090611
Send an email to the TXT contact email and the CAA contact email in the DNS. The email recipient clicks the link after the random number is expired.	3.2.2.4.13 3.2.2.4.14	Rejected	Satisfactory	2020-06-11 CR #1090611

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

Appedix D- Risks and Additional Controls

Risk

During the annual audit a particular risk pertaining to the segregation between the Public Certification Authority - G2 and the Public Certification Authority - G3 was identified. The nature of this risk is illustrated as follows:

The certificate profiles used by the Public Certification Authority - G2 and the Public Certification Authority - G3 were stored in the same directory. The value in a specific table determines which certificate profiles can be used by the Public Certification Authority - G2 or the Public Certification Authority - G3 to issue a specific type of certificates and the value can be changed by the system administrator through the CA management interface. Mistakes in the setting of the values of the mapping of the CAs to the certificate profiles may lead to the issuance of the certificates by the wrong CA. There is no control in place to prevent or detect this risk but no certificate was found to be mis-issued due to this matter.

Additional Controls

The following additional controls were proposed by CA System Vendor and CHT's operational team:

Control Objective	Control Design	Expected Deployment Date	How to evaluate the effectiveness
To avoid a specific type of certificates issued by the wrong CA	A Type-CA Configuration file is used to mandate the mapping between the types of certificates and the CAs.	2020/8/31	To conduct testing of the certificate issuance by the wrong combinations of the types of certificates and the CAs.
To Avoid certificates with certificate format not in compliance with the requirements of the CPS or Root Program being issued by the CAs.	An inspection function of the certificate format is used to check the certificate format of the certificates that are going to be issued.	Accomplished	To conduct testing of the certificate issuance wrong certificate format the types of certificates and the CAs.

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

Control Objective	Control Design	Expected Deployment Date	How to evaluate the effectiveness
To detect the change of the Type-CA Configuration file	The Type-CA Configuration file is to be stored in the directory which is already under the automatic daily check for the change of files and directories	The automatic daily check for the change of files and directories is an existing control	To make a change of the Type-CA Configuration file and to see if the alert of change is sent out.

中華電信

MANAGEMENT'S ASSERTION OF CHUNGHWA TELECOM

Chunghwa Telecom (CHT) operates the Certification Authority (CA) services known as CAs in Appendix A and provides SSL CA services.

CHT management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in CHT management's opinion, in providing its SSL and non-SSL CA services at Taipei and Taichung, Taiwan, throughout the period 1 June 2019 to 31 May 2020, CHT has:

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

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

- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and SSL certificates it manages is established and protected throughout their lifecycles; and
  - SSL certificate subscriber information is properly authenticated

- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorised individuals;
  - the continuity of key and certificate management operations is maintained; and

- CA systems development, maintenance, and operations are properly authorised and performed to maintain CA systems integrity

- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.4.1.

CHT disclosed publicly on the Mozilla's Bugzilla Platform the incident (Bug 1532436). In this incident, 2 certificates with unregistered FQDN were mis-issued. The details of the incident and the remediation taken by CHT were illustrated in Appendix C.

A particular risk pertaining to the segregation between the Public Certification Authority - G2 and the Public Certification Authority - G3 was identified during the audit process. No certificate was found to be mis-issued due to this matter. The nature of this risk and additional controls were illustrated in Appendix D.

Signature: PETER LIN

Title: Vice President

August 24, 2020

中華電信

Appendix A-List of CAs in Scope

Root CAs										
Common Name	**Subject**	**Issuer**	**Serial**	**Key Algorithm**	**Key Size**	**Sig. Algorithm**	**Not Before**	**Not After**	**SKI**	**SHA256 Fingerprint**
ePKI Root Certification Authority	OU = ePKI Root Certification Authority O = Chunghwa Telecom Co., Ltd. C = TW	OU = ePKI Root Certification Authority O = Chunghwa Telecom Co., Ltd. C = TW	15c8bd65475cafb897005ee406d2bc9d	rsaEncryption	4096 bits	sha1WithRSAEncryption	Dec 20 02:31:27 2004 GMT	Dec 20 02:31:27 2034 GMT	1e0cf7b667f2e192260945c055392e773f424aa2	c0a6f4dc63a24bfdcf54ef2a6a082a0a72de35803e2ff5ff527ae5d87206dfd5
ePKI Root Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G2	00d6962ec10a159312af8f63bcd444c95b	rsaEncryption	4096 bits	sha256WithRSAEncryption	Nov 17 08:23:42 2015 GMT	Dec 31 15:59:59 2037 GMT	725bbaaa7238ee259024b59422fa0988ca8b0afb	1e51942b84fd467bf77d1c89da241c04254dc8f3ef4c22451fe7a89978bdcd4f
ePKI Root Certification Authority - G3	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G3	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G3	6237e01b9aae4e4df86229bb44497b01	rsaEncryption	4096 bits	sha256WithRSAEncryption	Apr 30 09:42:34 2019 GMT	Dec 31 15:59:59 2037 GMT	51ce2e18aca1a4003549ba923bff095bbf3884ac	558fab7f4b5dff16b68ba4e40d1d3e940efa9b013350617d6f377c1724d9d421

中華電信

Root CAs										
Common Name	**Subject**	**Issuer**	**Serial**	**Key Algorithm**	**Key Size**	**Sig. Algorithm**	**Not Before**	**Not After**	**SKI**	**SHA256 Fingerprint**
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

Cross-Signed CA Certificates										
Common Name	**Subject**	**Issuer**	**Serial**	**Key Algorithm**	**Key Size**	**Sig. Algorithm**	**Not Before**	**Not After**	**SKI**	**SHA256 Fingerprint**
ePKI Root Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., OU=ePKI Root Certification Authority	3beee0918e8886ad460fe8ae910c9cba	rsaEncryption	4096 bits	sha256WithRSAEncryption	Nov 17 08:51:35 2015 GMT	Dec 20 02:31:27 2034 GMT	725bbaaa7238ee259024b59422fa0988ca8b0afb	64717250af8b028dd8e5c0bae4c9142c8b103532612bc487085fd3c319f9c067
ePKI Root Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., OU=ePKI Root Certification Authority	00afcd8d642c62d645067dc857fda8f15d	rsaEncryption	4096 bits	sha256WithRSAEncryption	Nov 17 08:51:35 2015 GMT	Dec 20 02:31:27 2034 GMT	725bbaaa7238ee259024b59422fa0988ca8b0afb	18467c4e64d586c844a44466de5ba7a6d5969c7a92859a511c5fdad75b03cdce

中華電信

Cross-Signed CA Certificates										
Common Name	**Subject**	**Issuer**	**Serial**	**Key Algorithm**	**Key Size**	**Sig. Algorithm**	**Not Before**	**Not After**	**SKI**	**SHA256 Fingerprint**
ePKI Root Certification Authority	C=TW, O=Chunghwa Telecom Co., Ltd., OU=ePKI Root Certification Authority	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G2	00cae1f73efcac5bb19c88c1c72f6f7b2f	rsaEncryption	4096 bits	sha256WithRSAEncryption	Nov 17 08:31:41 2015 GMT	Dec 20 02:31:27 2034 GMT	1e0cf7b667f2e192260945c055392e773f424aa2	d108c34a58c0e4a616449f8c48318023a229c86cd3ddd5d5fe6041a401c16a14
ePKI Root Certification Authority	C=TW, O=Chunghwa Telecom Co., Ltd., OU=ePKI Root Certification Authority	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G2	18907402b083ec8bce1994deafc0a1d7	rsaEncryption	4096 bits	sha256WithRSAEncryption	Nov 17 08:31:41 2015 GMT	Dec 20 02:31:27 2034 GMT	1e0cf7b667f2e192260945c055392e773f424aa2	b9c974de139f6308d74ccc423c3bc0bded5e7ab4ad738b304b50d429c42c3d66

OV SSL Issuing CAs										
Common Name	**Subject**	**Issuer**	**Serial**	**Key Algorithm**	**Key Size**	**Sig. Algorithm**	**Not Before**	**Not After**	**SKI**	**SHA256 Fingerprint**
Public Certification Authority	C=TW, O=Chunghwa Telecom Co., Ltd., OU=Public Certification Authority	C=TW, O=Chunghwa Telecom Co., Ltd., OU=ePKI Root Certification Authority	00c953feeeb895e91884abb22a68a42a7d	rsaEncryption	2048 bits	sha1WithRSAEncryption	May 16 10:13:55 2007 GMT	May 16 10:13:55 2027 GMT	71b35031a01b5b7bb2a6597cfd108c3cad3a3d7a	464b0ec0a602f0193db5f33911885a3a61921ad16d2664e25befab10cfa6ed25

中華電信

OV SSL Issuing CAs										
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	00973cc94d44cfe9a2e14f52e9a594a15a	rsaEncryption	2048 bits	sha1WithRSAEncryption	May 16 10:13:55 2007 GMT	May 16 10:13:55 2027 GMT	71b35031a01b5b7bb2a6597cfd108c3cad3a3d7a	4bd16f4955f3f3c9c8ea48ef9995324da5121724f89915d5f2c91eb0baef2337
Public Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., OU=Public Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., OU=ePKI Root Certification Authority	00c423d22191868fac4ee2fce4a011d1a7	rsaEncryption	2048 bits	sha256WithRSAEncryption	Dec 11 08:51:59 2014 GMT	Dec 11 08:51:59 2034 GMT	cb837d6515afa9c9f3a8a9f4647c795205744061	609930eb807ad420afda2a8aa61b67483039168cd766e09942a48bfe7f3bdc10
Public Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., OU=Public Certification Authority - G2	C=TW, O=Chunghwa Telecom Co., Ltd., OU=ePKI Root Certification Authority	143596f2441a7167983ffc9597419b53	rsaEncryption	2048 bits	sha256WithRSAEncryption	Dec 11 08:51:59 2014 GMT	Dec 11 08:51:59 2034 GMT	cb837d6515afa9c9f3a8a9f4647c795205744061	dae3434f696fc9f0f652e1b2a6f69b5e9273d09f43bd3bdd4717d6141f8cd2c2
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

中華電信

EV SSL Issuing CAs										
Common Name	**Subject**	**Issuer**	**Serial**	**Key Algorithm**	**Key Size**	**Sig. Algorithm**	**Not Before**	**Not After**	**SKI**	**SHA256 Fingerprint**
HiPKI EV TLS CA - G1	C=TW, O=Chunghwa Telecom Co., Ltd., CN=HiPKI EV TLS CA - G1	C=TW, O=Chunghwa Telecom Co., Ltd., CN=HiPKI Root CA - G1	3c43cdcddcf23b004f0ea073fc3ea389	rsaEncryption	4096 bits	sha256WithRSAEncryption	Feb 22 09:56:03 2019 GMT	Dec 31 15:59:59 2037 GMT	a90dea63aee38c0340e7ffdc3328e5238ecb109b	2a8e6a86e74d10edb2026c81693d64957a0f081c1631912ac95efdfcb5625657

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

Document Name	Version	Effective Date
ePKI CP	V1.8	November 18, 2019
ePKI CP	V1.75	August 12, 2019
ePKI CP	V1.7	April 30, 2019
eCA CPS	V1.7	April 22, 2020
eCA CPS	V1.67	November 18, 2019
eCA CPS	V1.65	August 30, 2019
eCA CPS	V1.6	April 30, 2019
PublicCA CPS	V2.0	April 22, 2020
PublicCA CPS	V1.9	April 30, 2019
HiPKI CP	V1.05	March 2, 2020
HiPKI CP	V1.0	February 22, 2019
HiPKI RCA CPS	V1.05	March 2, 2020
HiPKI RCA CPS	V1.0	February 22, 2019
EV TLS CA CPS	V1.05	March 2, 2020
EV TLS CA CPS	V1.0	February 22, 2019

中華電信

Appedix C- Incidents and Remediation

Incident

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

Bugzilla Number: Bug 1532436

Opened Date: March 4, 2019

Status: Open

Certificates Issued By: Public Certification Authority - G2

Description:

A certificate with unregistered FQDN www.raotest.com.tw was mis-issued on November 12, 2018 11:53:02 (UTC) and revoked on 15 February 2019 1:59; a certificate with unregistered FQDN publicca.rao.com.tw was mis-issued on January 29, 2019 06:43:59 (UTC) and revoked immediately. These two certificates were issued by the same RAO because the RAO intended to take a screenshot of certificate application process for training material.

Remediation

(1). To implement a two-stage manual verification by different RAOs.

This control has been in place since February 26, 2019.

(2). To implement an automatic FQDN-checking function.

This automatic FQDN-checking function went live on March 15, 2019.

The tested scenarios were summarized as follows:

Scenario	Expected Outcome	Test Result	Deployment Date and Change Request Number
Query the FQDN with WHOIS and find the applied-for FQDN is unregistered.	Rejected	Satisfactory	2019-03-15 CR # 1080315
Query the FQDN with WHOIS and find the applied-for FQDN is unregistered. The RAO modifies the status of the application ticket and triggers the issuance function.	Rejected	Satisfactory	2019-03-15 CR # 1080315

The test result indicated the function was satisfied.

(3). To implement an automatic domain control validation function.

Test cases were developed according to the functionality and the BR validation requirements. The test result indicated the function was satisfied.

The tested scenarios, the corresponding BR validation requirements and the deployment date were summarized as follows:

Scenario	BR Validation Requirement	Expected Outcome	Test Result	Deployment Date and Change Request Number
Query the FQDN with WHOIS. The Registrar is HINET and the organization name of the FQDN matches with the full name on the SSL application form.	3.2.2.4.12	Passed	Satisfactory	2020-02-19 CR #1090219
Query the FQDN with WHOIS. The Registrar is HINET but the organization name of the FQDN does not match with the full name on the SSL application form.	3.2.2.4.12	Rejected	Satisfactory	2020-02-19 CR #1090219
Query the FQDN with WHOIS. The Registrar is not HINET; The organization name of the FQDN matches with the full	3.2.2.4.2	Passed	Satisfactory	2020-06-22 CR #1090622-2

Scenario	BR Validation Requirement	Expected Outcome	Test Result	Deployment Date and Change Request Number
name on the SSL application form; and The Contact email of the FQDN matches with the technical person's email				
Query the FQDN with WHOIS. The Registrar is not HINET; The organization name of the FQDN matches with the full name on the SSL application form; and The Contact email of the FQDN does not match with the technical person's email	3.2.2.4.2	Rejected	Satisfactory	2020-06-22 CR #1090622-2
Query the FQDN with WHOIS. The Registrar is not HINET. The organization name of the FQDN does not match with the full name on the SSL application form.	3.2.2.4.2	Rejected	Satisfactory	2020-06-22 CR #1090622-2
Send an email to the technical person's email address on the SSL application form with a file containing a random value. Ask the person to put the file under the .well-known/pki-validation/ directory of the FQDN. The random value is correct and not expired.	3.2.2.4.6	Passed	Satisfactory	2020-02-19 CR #1090219
Send an email to the technical person's email address on the SSL application form with a file containing a random value. Ask the person to put the file under the .well-known/pki-validation/ directory of the FQDN. The file is missing.	3.2.2.4.6	Rejected	Satisfactory	2020-02-19 CR #1090219
Send an email to the technical person's email address on the	3.2.2.4.6	Rejected	Satisfactory	2020-02-19 CR #1090219

Scenario	BR Validation Requirement	Expected Outcome	Test Result	Deployment Date and Change Request Number
SSL application form with a file containing a random value. Ask the person to put the file under the .well-known/pki-validation/ directory of the FQDN. The random value is incorrect.				
Send an email to the technical person's email address on the SSL application form with a file containing a random value. Ask the person to put the file under the .well-known/pki-validation/ directory of the FQDN. The random value is correct but expired.	3.2.2.4.6	Rejected	Satisfactory	2020-02-19 CR #1090219
Send an email to the technical person's email address on the SSL application form with a file containing a random value. Ask the person to put the file under the .well-known/pki-validation/ directory of the FQDN. The URL is redirected to different website (http return code:3xx) The file can be found. The random value is correct and not expired.	3.2.2.4.18	Passed	Satisfactory	2020-05-25 CR #1090525
Send an email to the technical person's email address on the SSL application form with a file containing a random value. Ask the person to put the file under the .well-known/pki-validation/ directory of the FQDN. The URL is redirected to different page of the same website (http return code:3xx)	3.2.2.4.18	Passed	Satisfactory	2020-05-25 CR #1090525

Scenario	BR Validation Requirement	Expected Outcome	Test Result	Deployment Date and Change Request Number
The file can be found. The random value is correct and not expired.				
Send an email to the technical person's email address on the SSL application form with a file containing a random value. Ask the person to put the file under the .well-known/pki-validation/ directory of the FQDN. The URL is redirected to different website (http return code:3xx) The file can be found. The random value is incorrect.	3.2.2.4.18	Rejected	Satisfactory	2020-05-25 CR #1090525
Send an email to the technical person's email address on the SSL application form with a file containing a random value. Ask the person to put the file under the .well-known/pki-validation/ directory of the FQDN. The URL is redirected to different website (http return code:3xx) The file can be found. The random value is expired.	3.2.2.4.18	Rejected	Satisfactory	2020-05-25 CR #1090525
Send an email to the technical person's email address on the SSL application form with a file containing a random value. Ask the person to put the file under the .well-known/pki-validation/ directory of the FQDN. The URL is redirected to different page of the same website (http return code:3xx) The file cannot be found.	3.2.2.4.18	Rejected	Satisfactory	2020-05-25 CR #1090525

Scenario	BR Validation Requirement	Expected Outcome	Test Result	Deployment Date and Change Request Number
Send an email to the technical person's email address on the SSL application form with a file containing a random value. Ask the person to put the file under the .well-known/pki-validation/ directory of the FQDN. The URL is redirected to different page of the same website (http return code:3xx) The file can be found. The random value is incorrect .	3.2.2.4.18	Rejected	Satisfactory	2020-05-25 CR #1090525
Send an email to the technical person's email address on the SSL application form with a file containing a random value. Ask the person to put the file under the .well-known/pki-validation/ directory of the FQDN. The URL is redirected to different page of the same website (http return code:3xx) The file can be found. The random value is expired.	3.2.2.4.18	Rejected	Satisfactory	2020-05-25 CR #1090525
Send an email to the technical person's email address on the SSL application form with a random value in the content. Ask the person to put the random value in the DNS TXT Record by the required format.	3.2.2.4.7	Passed	Satisfactory	2019-06-10 CR #1080610-2
Send an email to the technical person's email address on the SSL application form with a random value in the content. Ask the person to put the random value in the DNS TXT Record by the required format.	3.2.2.4.7	Rejected	Satisfactory	2019-06-10 CR #1080610-2

Scenario	BR Validation Requirement	Expected Outcome	Test Result	Deployment Date and Change Request Number
The system periodically checks with the dig command and finds the value is incorrect.				
Send an email to the technical person's email address on the SSL application form with a random value in the content. Ask the person to put the random value in the DNS TXT Record by the required format. The system periodically checks with the dig command and finds the value is correct but expired.	3.2.2.4.7	Rejected	Satisfactory	2019-06-10 CR #1080610-2
Query the FQDN with WHOIS. Send an email to the registrant email with confirming link with the random value. The email recipient clicks the link and is directed to the authorization link. The email recipient clicks the authorization link.	3.2.2.4.2	Passed	Satisfactory	2020-06-22 CR #1090622-2
Query the FQDN with WHOIS. Send an email to the registrant email with confirming link of the random value. The email recipient modifies the link and clicks the link.	3.2.2.4.2	Rejected	Satisfactory	2020-06-22 CR #1090622-2
Query the FQDN with WHOIS. Send an email to the registrant email with confirming link of the random value. The email recipient clicks the link after 30 days.	3.2.2.4.2	Rejected	Satisfactory	2020-06-22 CR #1090622-2
Send an email to the postmaster, webmaster, hostmaster of the FQDN with confirming link of the random value. The email recipient clicks the link and is directed to the conformation webpage	3.2.2.4.4	Passed	Satisfactory	2020-02-19 CR #1090219

Scenario	BR Validation Requirement	Expected Outcome	Test Result	Deployment Date and Change Request Number
Send an email to the postmaster, webmaster, hostmaster of the FQDN with confirming link of the random value. The email recipient modifies the link and clicks the link.	3.2.2.4.4	Rejected	Satisfactory	2020-02-19 CR #1090219
Send an email to the postmaster, webmaster, hostmaster of the FQDN with confirming link of the random value. The email recipient clicks the link after 30 days.	3.2.2.4.4	Rejected	Satisfactory	2020-02-19 CR #1090219
Send an email to the TXT contact email and the CAA contact email in the DNS. The email recipient clicks the link and is directed to the confirmation webpage.	3.2.2.4.13 3.2.2.4.14	Passed	Satisfactory	2020-06-11 CR #1090611
Send an email to the TXT contact email and the CAA contact email in the DNS. The email recipient modifies the link and clicks the link.	3.2.2.4.13 3.2.2.4.14	Rejected	Satisfactory	2020-06-11 CR #1090611
Send an email to the TXT contact email and the CAA contact email in the DNS. The email recipient clicks the link after the random number is expired.	3.2.2.4.13 3.2.2.4.14	Rejected	Satisfactory	2020-06-11 CR #1090611

Appedix D- Risks and Additional Controls

Risk

During the annual audit a particular risk pertaining to the segregation between the Public Certification Authority - G2 and the Public Certification Authority - G3 was identified. The nature of this risk is illustrated as follows:

The certificate profiles used by the Public Certification Authority - G2 and the Public Certification Authority - G3 were stored in the same directory. The value in a specific table determines which certificate profiles can be used by the Public Certification Authority - G2 or the Public Certification Authority - G3 to issue a specific type of certificates and the value can be changed by the system administrator through the CA management interface. Mistakes in the setting of the values of the mapping of the CAs to the certificate profiles may lead to the issuance of the certificates by the wrong CA. There is no control in place to prevent or detect this risk but no certificate was found to be mis-issued due to this matter.

Additional Controls

The following additional controls were proposed by CA System Vendor and CHT's operational team:

Control Objective	Control Design	Expected Deployment Date	How to evaluate the effectiveness
To avoid a specific type of certificates issued by the wrong CA	A Type-CA Configuration file is used to mandate the mapping between the types of certificates and the CAs.	2020/8/31	To conduct testing of the certificate issuance by the wrong combinations of the types of certificates and the CAs.

Control Objective	Control Design	Expected Deployment Date	How to evaluate the effectiveness
To Avoid certificates with certificate format not in compliance with the requirements of the CPS or Root Program being issued by the CAs.	An inspection function of the certificate format is used to check the certificate format of the certificates that are going to be issued.	Accomplished	To conduct testing of the certificate issuance wrong certificate format the types of certificates and the CAs.
To detect the change of the Type-CA Configuration file	The Type-CA Configuration file is to be stored in the directory which is already under the automatic daily check for the change of files and directories	The automatic daily check for the change of files and directories is an existing control	To make a change of the Type-CA Configuration file and to see if the alert of change is sent out.

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 (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 2019 to 31 May 2020 for its CAs as enumerated in Appendix A, 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 Principle 4 of the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.4.1.

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 Principle 4 of the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.4.1.

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 Control 1, 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 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 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 2019 to 31 May 2020, CHT management's assertion, as referred to above, is fairly stated, in all material respects, in accordance with Principle 4 of the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.4.1.

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

This report does not include any representation as to the quality of CHT's services beyond those covered by Principle 4 of the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.4.1, nor the suitability of any of CHT's services for any customer's intended purpose.

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

August 24, 2020

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

Other CAs										
Common Name	**Subject**	**Issuer**	**Serial**	**Key Algorithm**	**Key Size**	**Sig. Algorithm**	**Not Before**	**Not After**	**SKI**	**SHA256 Fingerprint**
Public Certification Authority - G3	C=TW, O=Chunghwa Telecom Co., Ltd., CN=Public Certification Authority - G3	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G3	0088c1807ba0abb62e1f49a42a028be43e	rsaEncryption	2048 bits	sha256WithRSAEncryption	Apr 30 09:52:26 2019 GMT	Dec 31 15:59:59 2037 GMT	7b6b4b5754a5bb5d1a081ee986ec203b3951287c	b0f1f7c7df837bdf88825a444444e4815da7e0899728a07ae8767d5f65b50995

中華電信

MANAGEMENT'S ASSERTION OF CHUNGHWA TELECOM

Chunghwa Telecom (CHT) operates the Certification Authority (CA) services known as CAs in Appendix A and provides non-SSL CA services.

CHT management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in CHT management's opinion, in providing its non-SSL CA services at Taipei and Taichung, Taiwan, throughout the period 1 June 2019 to 31 May 2020, 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 Principle 4 of the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.4.1.

Signature: PETER LIN

Title: Vice President

August 24, 2020

中華電信

Appendix A-List of CAs in Scope

Timestamp CA										
Common Name	**Subject**	**Issuer**	**Serial**	**Key Algorithm**	**Key Size**	**Sig. Algorithm**	**Not Before**	**Not After**	**SKI**	**SHA256 Fingerprint**
Public Certification Authority - G3	C=TW, O=Chunghwa Telecom Co., Ltd., CN=Public Certification Authority - G3	C=TW, O=Chunghwa Telecom Co., Ltd., CN=ePKI Root Certification Authority - G3	0088c1807ba0abb62e1f49a42a028be43e	rsaEncryption	2048 bits	sha256WithRSAEncryption	Apr 30 09:52:26 2019 GMT	Dec 31 15:59:59 2037 GMT	7b6b4b5754a5bb5d1a081ee986ec203b3951287c	b0f1f7c7df837bdf88825a444444e4815da7e0899728a07ae8767d5f65b50995

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

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

INDEPENDENT ASSURANCE REPORT

To the management of Chunghwa Telecom (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 18 October 2019 to 31 May 2020 for its CAs as enumerated in Appendix A, 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 Principle 4 of the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.4.1.

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 Principle 4 of the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.4.1.

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 Control 1, 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 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 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 18 October 2019 to 31 May 2020, CHT management's assertion, as referred to above, is fairly stated, in all material respects, in accordance with Principle 4 of the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.4.1.

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

This report does not include any representation as to the quality of CHT's services beyond those covered by Principle 4 of the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.4.1, nor the suitability of any of CHT's services for any customer's intended purpose.

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

August 24, 2020

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

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 7d0d67c6 3874844f 8461c5f4 b54	rsaEncryption	4096 bits	sha256WithRSAEncryption	Oct 18 02:50:29 2019 GMT	Dec 29 16:00:00 2037 GMT	d696a2d5966 e2d3e40b1a3 b26d88777bf 6d6f4ca	da31293d659781c6 9e0085c732a2811d b50e5cc576909149 b80a98a9b0f93fd9

中華電信

MANAGEMENT'S ASSERTION OF CHUNGHWA TELECOM

Chunghwa Telecom (CHT) operates the Certification Authority (CA) services known as CAs in Appendix A and provides non-SSL CA services.

CHT management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in CHT management's opinion, in providing its non-SSL CA services at Taipei and Taichung, Taiwan, throughout the period 18 October 2019 to 31 May 2020, 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 Principle 4 of the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.4.1.

Signature: PETER LIN

Title: Vice President

August 24, 2020

中華電信

Appendix A-List of CAs in Scope

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 7d0d67c6 3874844f 8461c5f4 b54	rsaEncryption	4096 bits	sha256WithRS AEncryption	Oct 18 02:50:29 2019 GMT	Dec 29 16:00:00 2037 GMT	d696a2d5966 e2d3e40b1a3 b26d88777bf 6d6f4ca	da31293d659781c6 9e0085c732a2811d b50e5cc576909149 b80a98a9b0f93fd9