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

REPORT OF THE INDEPENDENT ACCOUNTANT

To the management of Chunghwa Telecom:

We have examined the assertion by the management of Chunghwa Telecom(CHT) that in providing its Extended Validation(EV) SSL certification authority(CA) services at Taipei and Taichung, Taiwan, during the period from June 1, 2017 through May 31, 2018 for its ePKI EV SSL CA listed in Appendix A, CHT has:

- Disclosed its EV Certificate life cycle management practices and procedures, including its commitment to provide EV Certificates in conformity with the CA/Browser Forum Guidelines, and provided such services in accordance with its applicable disclosed practices in its certification practice statements and certificate policies listed in Appendix B
- Maintained effective controls to provide reasonable assurance that:
  - EV Subscriber information was properly collected, authenticated (for the registration activities performed by CHT) and verified, and
  - The integrity of keys and EV certificates it manages was established and protected throughout their life cycles

based on WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL – Version 1.6.0.

CHT's management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included (1) obtaining an understanding CHT's EV certificate life cycle management practices and procedures, including its relevant controls over the issuance, renewal and revocation of EV certificates; (2) evaluating the suitability of the design of practices and procedures; and (3) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

In our opinion, CHT management's assertion, as referred to above, is fairly stated, in all material respects, based on the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL – Version 1.6.0.

Because of inherent limitations in controls, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that (1) changes made to the system or controls, (2) changes in processing requirements, (3) changes required because of the passage of time, or (4) degree of compliance with the policies or procedures may alter the validity of such conclusions.

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.

CHT's use of the WebTrust for CAs EV 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

July 9, 2018

DFK INTERNATIONAL

Appendix A – ePKI Root and EV SSL CA within the Audit Report Scope

eCA	**Root CA Certificate**	
	Subject	Issuer

	OU = ePKI Root Certification Authority
	O = Chunghwa Telecom Co., Ltd.
	C = TW
		OU = ePKI Root Certification Authority
		O = Chunghwa Telecom Co., Ltd.
		C = TW

	Certificate Related Information	Key Related Information
	Serial Number: 15 c8 bd 65 47 5c af b8 97 00 5e e4 06 d2 bc 9d Signature Algorithm: sha1RSA Not Before: 2004-12-20 10:31:27 a.m. (UTC +8:00) Not After : 2034-12-20 10:31:27 a.m. (UTC +8:00) Thumbprint Algorithm: sha1 Thumbprint: 67:65:0D:F1:7E:8E:7E:5B:82:40:A4:F4:56:4B:CF:E2:3D:69:C6:F0 Thumbprint Algorithm: sha256 C0:A6:F4:DC:63:A2:4B:FD:CF:54:EF:2A:6A:08:2A:0A:72:DE:35:80:3E:2F:F5:FF:52:7A:E5:D8:72:06:DF:D5	Subject Public Key: RSA(4096 bits) Subject Key Identifiers: 1e 0c f7 b6 67 f2 e1 92 26 09 45 c0 55 39 2e 77 3f 42 4a a2
	Additional Information	Remark
		■ Self-signed by 1st Generation of ePKI Root Certification Authority.
eCA - G2	**Root CA Certificate**	
	Subject	Issuer

	CN = ePKI Root Certification Authority - G2
	O = Chunghwa Telecom Co., Ltd.
	C = TW
		CN = ePKI Root Certification Authority - G2
		O = Chunghwa Telecom Co., Ltd.
		C = TW

	Certificate Related Information	Key Related Information
	Serial Number: 00 d6 96 2e c1 0a 15 93 12 af 8f 63 bc d4 44 c9 5b Signature Algorithm: sha256RSA Not Before: 2015-11-17 04:23:42 p.m. (UTC +8:00) Not After : 2037-12-31 11:59:59 p.m. (UTC +8:00) Thumbprint Algorithm: sha1	Subject Public Key: RSA(4096 bits) Subject Key Identifiers: 72 5b ba aa 72 38 ee 25 90 24 b5 94 22 fa 09 88 ca 8b 0a fb Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)

	Thumbprint: D9:9B:10:42:98:59:47:63:F0:B9:A9:27:B7:92:69:CB:47:DD:15:8B Thumbprint Algorithm: sha256 1E:51:94:2B:84:FD:46:7B:F7:7D:1C:89:DA:24:1C:04:25:4D:C8:F3:EF:4C:22:45:1F:E7:A8:99:78:BD:CD:4F	
	Additional Information	Remark
		■ Self-signed by 2nd Generation of ePKI Root Certification Authority.
ePKI EV SSL CA	**Intermediate CA Certificate**	
	Subject	Issuer

	CN = ePKI EV SSL Certification Authority - G1
	O = Chunghwa Telecom Co., Ltd.
	C = TW
		CN = ePKI Root Certification Authority - G2
		O = Chunghwa Telecom Co., Ltd.
		C = TW

	Certificate related Information	Key Related Information
	Serial Number: 00 f7 4e 18 0c 99 e2 7b 8d 9f 79 4f b1 b7 c0 bf 48 Signature Algorithm: sha256RSA Not Before: 2016-02-04 11:06:31 a.m. (UTC +8:00) Not After : 2030-02-04 11:06:31 a.m. (UTC +8:00) Thumbprint Algorithm: sha1 Thumbprint: 81:AC:5D:E1:50:D1:B8:DE:5D:3E:0E:26:6A:13:6B:73:78:62:D3:22 Thumbprint Algorithm: sha256 Thumbprint: BE:BC:E5:7D:CB:85:F6:0A:93:BF:A5:01:9E:DB:1A:29:4B:F6:D8:1F:82:D9:B4:E7:1F:50:2F:0B:15:A1:FC:08	Subject Public Key: RSA(2048 bits) Authority Key Identifiers: 72 5b ba aa 72 38 ee 25 90 24 b5 94 22 fa 09 88 ca 8b 0a fb Subject Key Identifiers: 59 38 aa 5b 50 81 ec d2 28 0a 37 e3 0a a4 06 84 a9 92 99 39 Basic Constraint: Subject Type=CA Path Length Constraint=0 Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)
	Additional Information	Remark
	CRL Distribution Point: http://eca.hinet.net/repository/CRL2/CA.crl Certificate Policy: [1]2.23.140.1.1	■ CA certificate of ePKI EV SSL Certification Authority - G1 was signed by eCA - G2 on 2016-02-04. ■ CA certificate was published in the repository : http://eca.hinet.net/en/repository_c2.htm ■ News of the publication of CA certificate was announced on 2016/02/16 : http://eca.hinet.net/en/index.htm then moved to : https://eca.hinet.net/en/history.htm

		■ Approved CPS v1.2 was published in the repository: http://eca.hinet.net/en/repository_a.htm ■ Readiness assessment of ePKI EV SSL CA against CPS v1.1, WebTrust Principles and Criteria for Certification Authorities 2.0, WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.0, and WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL – Version 1.4.5 has been accomplished on December 27, 2016.

Appendix B – Applicable Certification Practice Statements and Certificate Policies during the Audit Period.

Document	Version	Effective Date
ePKI CP	1.6	May 28, 2018
ePKI CP	1.5	December 1, 2017
ePKI CP	1.4	September 23, 2016
eCA CPS	1.5	May 28, 2018
eCA CPS	1.4	March 14, 2018
eCA CPS	1.4(20180214)	February 14, 2018
eCA CPS	1.4(20180126)	January 26, 2018
eCA CPS	1.4(20171023)	October 23, 2017
eCA CPS	1.4(20170714)	July 14, 2017
eCA CPS	1.3	February 4, 2016
ePKI EV SSL CA CPS	1.2	May 28, 2018
ePKI EV SSL CA CPS	1.1	March 14, 2018
ePKI EV SSL CA CPS	1.1 (20180214)	February 14, 2018
ePKI EV SSL CA CPS	1.1 (20180126)	January 26, 2018
ePKI EV SSL CA CPS	1.1 (20171023)	October 23, 2017
ePKI EV SSL CA CPS	1.1 (20170714)	July 14, 2017
ePKI EV SSL CA CPS	1.0	July 26, 2016

*The documents listed above are available online at the following addresses:

http://eca.hinet.net/en/repository_a.htm or http://eca.hinet.net/en/repository_d.htm

中華電信

Assertion of Management as to its Disclosure of its Business Practices and its Controls Over its Certification Authority Operations During the Period from June 1, 2017 through May 31, 2018

July 9, 2018

The management of Chunghwa Telecom (CHT) has assessed the controls over its Extended Validation(EV) SSL Certification Authority(CA) services located at Taipei and Taichung, Taiwan. Based on that assessment, in CHT Management's opinion, in providing its ePKI EV SSL CA services at Taipei and Taichung, Taiwan, during the period from June 1, 2017 through May 31, 2018 for its ePKI EV SSL CA listed in Appendix A, CHT has:

- Disclosed its EV Certificate life cycle management practices and procedures, including its commitment to provide EV Certificates in conformity with the CA/Browser Forum Guidelines, and provided such services in accordance with disclosed practices in its certification practice statements and certificate policies listed in Appendix B
- Maintained effective controls to provide reasonable assurance that:
  - EV Subscriber information was properly collected, authenticated (for the registration activities performed by CHT) and verified, and
  - The integrity of keys and EV certificates it managed was established and protected throughout their life cycles

in accordance with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL – Version 1.6.0.

Signature: Chung, Ming

Title: Principle Engineer

Appendix A – ePKI Root and EV SSL CA within the Audit Report Scope

eCA	**Root CA Certificate**	
	Subject	Issuer

	OU = ePKI Root Certification Authority
	O = Chunghwa Telecom Co., Ltd.
	C = TW
		OU = ePKI Root Certification Authority
		O = Chunghwa Telecom Co., Ltd.
		C = TW

	Certificate Related Information	Key Related Information
	Serial Number: 15 c8 bd 65 47 5c af b8 97 00 5e e4 06 d2 bc 9d Signature Algorithm: sha1RSA Not Before: 2004-12-20 10:31:27 a.m. (UTC +8:00) Not After : 2034-12-20 10:31:27 a.m. (UTC +8:00) Thumbprint Algorithm: sha1 Thumbprint: 67:65:0D:F1:7E:8E:7E:5B:82:40:A4:F4:56:4B:CF:E2:3D:69:C6:F0 Thumbprint Algorithm: sha256 C0:A6:F4:DC:63:A2:4B:FD:CF:54:EF:2A:6A:08:2A:0A:72:DE:35:80:3E:2F:F5:FF:52:7A:E5:D8:72:06:DF:D5	Subject Public Key: RSA(4096 bits) Subject Key Identifiers: 1e 0c f7 b6 67 f2 e1 92 26 09 45 c0 55 39 2e 77 3f 42 4a a2
	Additional Information	Remark
		■ Self-signed by 1st Generation of ePKI Root Certification Authority.
eCA - G2	**Root CA Certificate**	
	Subject	Issuer

	CN = ePKI Root Certification Authority - G2
	O = Chunghwa Telecom Co., Ltd.
	C = TW
		CN = ePKI Root Certification Authority - G2
		O = Chunghwa Telecom Co., Ltd.
		C = TW

	Certificate Related Information	Key Related Information
	Serial Number: 00 d6 96 2e c1 0a 15 93 12 af 8f 63 bc d4 44 c9 5b Signature Algorithm: sha256RSA Not Before: 2015-11-17 04:23:42 p.m. (UTC +8:00) Not After : 2037-12-31 11:59:59 p.m. (UTC +8:00) Thumbprint Algorithm: sha1	Subject Public Key: RSA(4096 bits) Subject Key Identifiers: 72 5b ba aa 72 38 ee 25 90 24 b5 94 22 fa 09 88 ca 8b 0a fb Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)

	Thumbprint: D9:9B:10:42:98:59:47:63:F0:B9:A9:27:B7:92:69:CB:47:DD:15:8B Thumbprint Algorithm: sha256 1E:51:94:2B:84:FD:46:7B:F7:7D:1C:89:DA:24:1C:04:25:4D:C8:F3:EF:4C:22:45:1F:E7:A8:99:78:BD:CD:4F	
	Additional Information	Remark
		■ Self-signed by 2nd Generation of ePKI Root Certification Authority.
ePKI EV SSL CA	**Intermediate CA Certificate**	
	Subject	Issuer

	CN = ePKI EV SSL Certification Authority - G1
	O = Chunghwa Telecom Co., Ltd.
	C = TW
		CN = ePKI Root Certification Authority - G2
		O = Chunghwa Telecom Co., Ltd.
		C = TW

	Certificate related Information	Key Related Information
	Serial Number: 00 f7 4e 18 0c 99 e2 7b 8d 9f 79 4f b1 b7 c0 bf 48 Signature Algorithm: sha256RSA Not Before: 2016-02-04 11:06:31 a.m. (UTC +8:00) Not After : 2030-02-04 11:06:31 a.m. (UTC +8:00) Thumbprint Algorithm: sha1 Thumbprint: 81:AC:5D:E1:50:D1:B8:DE:5D:3E:0E:26:6A:13:6B:73:78:62:D3:22 Thumbprint Algorithm: sha256 Thumbprint: BE:BC:E5:7D:CB:85:F6:0A:93:BF:A5:01:9E:DB:1A:29:4B:F6:D8:1F:82:D9:B4:E7:1F:50:2F:0B:15:A1:FC:08	Subject Public Key: RSA(2048 bits) Authority Key Identifiers: 72 5b ba aa 72 38 ee 25 90 24 b5 94 22 fa 09 88 ca 8b 0a fb Subject Key Identifiers: 59 38 aa 5b 50 81 ec d2 28 0a 37 e3 0a a4 06 84 a9 92 99 39 Basic Constraint: Subject Type=CA Path Length Constraint=0 Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)
	Additional Information	Remark
	CRL Distribution Point: http://eca.hinet.net/repository/CRL2/CA.crl Certificate Policy: [1]2.23.140.1.1	■ CA certificate of ePKI EV SSL Certification Authority - G1 was signed by eCA - G2 on 2016-02-04. ■ CA certificate was published in the repository : http://eca.hinet.net/en/repository_c2.htm ■ News of the publication of CA certificate was announced on 2016/02/16 : http://eca.hinet.net/en/index.htm then moved to : https://eca.hinet.net/en/history.htm

		■ Approved CPS v1.2 was published in the repository: http://eca.hinet.net/en/repository_a.htm ■ Readiness assessment of ePKI EV SSL CA against CPS v1.1, WebTrust Principles and Criteria for Certification Authorities 2.0, WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security – Version 2.0, and WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL – Version 1.4.5 has been accomplished on December 27, 2016.

Appendix B – Applicable Certification Practice Statements and Certificate Policies during the Audit Period.

Document	Version	Effective Date
ePKI CP	1.6	May 28, 2018
ePKI CP	1.5	December 1, 2017
ePKI CP	1.4	September 23, 2016
eCA CPS	1.5	May 28, 2018
eCA CPS	1.4	March 14, 2018
eCA CPS	1.4(20180214)	February 14, 2018
eCA CPS	1.4(20180126)	January 26, 2018
eCA CPS	1.4(20171023)	October 23, 2017
eCA CPS	1.4(20170714)	July 14, 2017
eCA CPS	1.3	February 4, 2016
ePKI EV SSL CA CPS	1.2	May 28, 2018
ePKI EV SSL CA CPS	1.1	March 14, 2018
ePKI EV SSL CA CPS	1.1 (20180214)	February 14, 2018
ePKI EV SSL CA CPS	1.1 (20180126)	January 26, 2018
ePKI EV SSL CA CPS	1.1 (20171023)	October 23, 2017
ePKI EV SSL CA CPS	1.1 (20170714)	July 14, 2017
ePKI EV SSL CA CPS	1.0	July 26, 2016

*The documents listed above are available online at the following addresses:

http://eca.hinet.net/en/repository_a.htm or http://eca.hinet.net/en/repository_d.htm