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 certification authority(CA) services at Taipei and Taichung, Taiwan for its CA operation during the period from June 1, 2017 through May 31, 2018 for its ePKI Root and Intermediate CAs listed in Appendix A, CHT has:

- Disclosed its business, key life cycle management, certificate life cycle management, and CA environmental control practices in its certification practice statements and certificate policies listed in Appendix B
- Maintained effective controls to provide reasonable assurance that:
  - The CA's certification practice statement is consistent with its certificate policy; and
  - The CA provides its services in accordance with its certificate policy and certification practice statement
- Maintained effective controls to provide reasonable assurance that:
  - The integrity of keys and certificates it manages was established and protected throughout their life cycles; and
  - Subordinate CA certificate requests are accurate, authenticated and approved
- Maintained effective controls to provide reasonable assurance that:
  - Logical and physical access to CA systems and data was restricted to authorized individuals;

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

- The continuity of key and certificate management operations is maintained; and
- CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity

based on the Trust Service Principles and Criteria for Certification Authorities Version 2.0.

The management of CHT is responsible for its assertion. Our responsibility is to express an opinion on management 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:

- Obtaining an understanding of CHT's business, key life cycle management, certificate life cycle management, and CA environmental control practices
- Obtaining an understanding of the controls over:
  - The consistency of CA's certification practice statement with its certificate policy;
  - The compliance of CA's services in accordance with its disclosed practices;
  - Key and certificate integrity;
  - The authenticity and privacy of subscriber and relying party information;
  - Logical and physical access to CA systems and data;
  - The continuity of key and certificate life cycle management operations; 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

- Development, maintenance and operations of CA system integrity

- Selectively testing transactions executed in accordance with the management of disclosed key and certificate life cycle management business and information privacy practices
- Testing and evaluating the operating effectiveness of the controls
- 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, for the period from June 1, 2017 through May 31, 2018, CHT's management assertion, as set forth above, is fairly stated, in all material respects, based on the Trust Service Principles and Criteria for Certification Authorities Version 2.0.

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) the 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.

This report does not include any representation as to the quality of CHT's services beyond those covered by the Trust Service Principles and Criteria

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

for Certification Authorities Version 2.0, nor the suitability of any of CHT's services for any customer's intended purpose.

The WebTrust seal of assurance for Certification Authorities on CHT's website 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

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 – ePKI Root and Intermediate CAs 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)

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

	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.
eCA cross-signed by eCA – G2	**Self-Issued Certificate**	
	Subject	Issuer
	OU = ePKI Root Certification Authority 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 ca e1 f7 3e fc ac 5b b1 9c 88 c1 c7 2f 6f 7b 2f Signature Algorithm: sha256RSA Not Before: 2015-11-17 04:31:41 p.m. (UTC +8:00) Not After : 2034-12-20 10:31:27 a.m. (UTC +8:00) Thumbprint Algorithm: sha1 Thumbprint: DD:FE:11:1B:8A:9D:C4:76:10:81:19:2F:40:E7:C9:DA:1C:D3:D4:50 Thumbprint Algorithm: sha256 Thumbprint: D1:08:C3:4A:58:C0:E4:A6:16:44:9F:8C:48:31:80:23:A2:29:C8:6C:D3:DD:D5:D5:FE:60:41:A4:01:C1:6A:14	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
	Certificate Policy: [1]1.3.6.1.4.1.23459.100.0.1 [2]1.3.6.1.4.1.23459.100.0.2 [3]1.3.6.1.4.1.23459.100.0.3 [4]1.3.6.1.4.1.23459.100.0.4 [5]1.3.6.1.4.1.23459.100.0.9 [6]1.3.6.1.4.1.23459.100.0.0 [7]2.16.886.1.100.0.1	■ Self-issued certificates are generated to support changes in policy or operations following industry standards such as RFC 5280. ■ This certificate is 1st generation of ePKI Root CA public key with other subject information signed by 2nd generation of ePKI Root CA private key. It is for

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

	[8]2.16.886.1.100.0.2 [9]2.16.886.1.100.0.3 [10]2.16.886.1.100.0.4 [11]2.16.886.1.100.0.0 [12]2.23.140.1.2.1 [13]2.23.140.1.2.2 [14]2.23.140.1.2.3 [15]2.23.140.1.1	constructing trust path of 1st generation & 2nd generation of ePKI Root CA key pairs.
eCA - G2 cross-signed by eCA	**Self-Issued Certificate**	
	Subject	Issuer
	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
	Certificate related Information	Key Related Information
	Serial Number: 3b ee e0 91 8e 88 86 ad 46 0f e8 ae 91 0c 9c ba Signature Algorithm: sha256RSA Not Before: 2015-11-17 04:31:41 p.m. (UTC +8:00) Not After : 2034-12-20 10:31:27 a.m. (UTC +8:00) Thumbprint Algorithm: sha1 Thumbprint: C3:CA:F8:57:0C:B1:2D:D0:FC:97:37:BF:CD:0F:08:7C:9B:E6:D2:81 Thumbprint Algorithm: sha256 Thumbprint: 64:71:72:50:AF:8B:02:8D:D8:E5:C0:BA:E4:C9:14:2C:8B:10:35:32:61:2B:C4:87:08:5F:D3:C3:19:F9:C0:67	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
	Additional Information	Remark
	Certificate Policy: [1]1.3.6.1.4.1.23459.100.0.1 [2]1.3.6.1.4.1.23459.100.0.2 [3]1.3.6.1.4.1.23459.100.0.3 [4]1.3.6.1.4.1.23459.100.0.4 [5]1.3.6.1.4.1.23459.100.0.9 [6]1.3.6.1.4.1.23459.100.0.0 [7]2.16.886.1.100.0.1 [8]2.16.886.1.100.0.2 [9]2.16.886.1.100.0.3 [10]2.16.886.1.100.0.4	■ Self-issued certificates are generated to support changes in policy or operations following industry standards such as RFC 5280. ■ This certificate is 2nd generation of ePKI Root CA public key with other subject information signed by 1st generation of ePKI Root CA private key. It is for constructing trust path of 1st generation & 2nd generation of ePKI Root CA key pairs.

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

	[11]2.16.886.1.100.0.0 [12]2.23.140.1.2.1 [13]2.23.140.1.2.2 [14]2.23.140.1.2.3 [15]2.23.140.1.1	
PublicCA	**Intermediate CA Certificate**	
	Subject	Issuer
	OU = Public 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: 00 c9 53 fe ee b8 95 e9 18 84 ab b2 2a 68 a4 2a 7d Signature Algorithm: sha1RSA Not Before: 2007-05-16 06:13:55 p.m. (UTC +8:00) Not After : 2027-05-16 06:13:55 p.m. (UTC +8:00) Thumbprint Algorithm: sha1 Thumbprint: 40:FE:0D:8D:9F:99:8A:46:71:F5:C3:26:E5:3F:76:DB:85:59:C2:4F Thumbprint Algorithm: sha256 Thumbprint: 46:4B:0E:C0:A6:02:F0:19:3D:B5:F3:39:11:88:5A:3A:61:92:1A:D1:6D:26:64:E2:5B:EF:AB:10:CF:A6:ED:25	Subject Public Key: RSA(2048 bits) Authority Key Identifiers: 1e 0c f7 b6 67 f2 e1 92 26 09 45 c0 55 39 2e 77 3f 42 4a a2 Subject Key Identifiers: 71 b3 50 31 a0 1b 5b 7b b2 a6 59 7c fd 10 8c 3c ad 3a 3d 7a 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/CRL/CA.crl Certificate Policy: [1]2.16.886.1.100.0.1 [2]2.16.886.1.100.0.2 [3]2.16.886.1.100.0.3	■ CA certificate of 1st Generation of Public Certification Authority signed by eCA.
PublicCA	**Intermediate CA Certificate**	
	Subject	Issuer
	OU = Public Certification Authority O = Chunghwa Telecom Co., Ltd. C = TW	OU = ePKI Root Certification Authority O = Chunghwa Telecom Co., Ltd. C = TW

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

	Certificate related Information	Key Related Information
	Serial Number: 00 97 3c c9 4d 44 cf e9 a2 e1 4f 52 e9 a5 94 a1 5a Signature Algorithm: sha1RSA Not Before: 2007-05-16 06:13:55 p.m. (UTC +8:00) Not After : 2027-05-16 06:13:55 p.m. (UTC +8:00) Thumbprint Algorithm: sha1 Thumbprint: D6:D5:C7:92:AD:6B:2E:3A:B9:B4:23:01:4E:1B:40:E5:76:D8:EC:BF Thumbprint Algorithm: sha1 Thumbprint: 40:FE:0D:8D:9F:99:8A:46:71:F5:C3:26:E5:3F:76:DB:85:59:C2:4F Thumbprint Algorithm: sha256 Thumbprint: 46:4B:0E:C0:A6:02:F0:19:3D:B5:F3:39:11:88:5A:3A:61:92:1A:D1:6D:26:64:E2:5B:EF:AB:10:CF:A6:ED:25	Subject Public Key: RSA(2048 bits) Authority Key Identifiers: 1e 0c f7 b6 67 f2 e1 92 26 09 45 c0 55 39 2e 77 3f 42 4a a2 Subject Key Identifiers: 71 b3 50 31 a0 1b 5b 7b b2 a6 59 7c fd 10 8c 3c ad 3a 3d 7a 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/CRL/CA.crl Certificate Policy: [1]1.3.6.1.4.1.23459.100.0.1 [2]1.3.6.1.4.1.23459.100.0.2 [3]1.3.6.1.4.1.23459.100.0.3 [4]2.16.886.1.100.0.1 [5]2.16.886.1.100.0.2 [6]2.16.886.1.100.0.3 [7]2.23.140.1.2.1 [8]2.23.140.1.2.2	■ CA certificate of 1st Generation of Public Certification Authority signed by eCA. ■ To add the Organization Validation/Domain Validation CP OID adopted by CA/Browser Forum and CP OID with Private Enterprise Number of CHT.
PublicCA - G2	**Intermediate CA Certificate**	
	Subject	Issuer
	OU = Public Certification Authority - G2 O = Chunghwa Telecom Co., Ltd. C = TW	OU = ePKI Root Certification Authority - G2 O = Chunghwa Telecom Co., Ltd. C = TW

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

	Certificate related Information	Key Related Information
	Serial Number: 00 ce 60 97 fd 33 e1 2d a0 75 ce dc 96 5d c0 c4 a3 Signature Algorithm: sha256RSA Not Before: 2014-12-11 04:51:59 p.m. (UTC +8:00) Not After : 2034-12-11 04:51:59 p.m. (UTC +8:00) Thumbprint Algorithm: sha1 Thumbprint: DD:B1:3C:36:50:3D:BA:D9:4A:B0:B2:E3:89:E3:BB:F4:91:31:3E:5F Thumbprint Algorithm: sha256 Thumbprint: F5:FB:67:C8:45:3E:DA:34:DB:EC:8A:76:65:74:F0:7A:03:54:8C:08:4A:F2:F5:E6:45:5E:A7:69:60:8D:9A:D5	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: cb 83 7d 65 15 af a9 c9 f3 a8 a9 f4 64 7c 79 52 05 74 40 61 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]1.3.6.1.4.1.23459.100.0.1 [2]1.3.6.1.4.1.23459.100.0.2 [3]1.3.6.1.4.1.23459.100.0.3 [4]1.3.6.1.4.1.23459.100.0.9 [5]2.16.886.1.100.0.1 [6]2.16.886.1.100.0.2 [7]2.16.886.1.100.0.3 [8]2.23.140.1.2.1 [9]2.23.140.1.2.2 [10]2.23.140.1.2.3	■ CA certificate of 2nd Generation of Public Certification Authority signed by ePKI Root Certification Authority - G2. ■ Add 1.3.6.1.4.1.23459.100.0.9 CP OID in Certificate Policy extension for PDF Signing. ■ CA certificate was published in the repository : http://eca.hinet.net/en/repository_c2.htm#PublicCA_CA2 ■ News of the publication of CA certificate was announced on 2016/10/13 : http://eca.hinet.net/en/index.htm , then moved to : https://eca.hinet.net/en/history.htm
PublicCA - G2	**Intermediate CA Certificate**	
	Subject	Issuer
	OU = Public Certification Authority - G2 O = Chunghwa Telecom Co., Ltd. C = TW	OU = ePKI Root Certification Authority O = Chunghwa Telecom Co., Ltd. C = TW

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

	Certificate related Information	Key Related Information
	Serial Number: 00 c4 23 d2 21 91 86 8f ac 4e e2 fc e4 a0 11 d1 a7 Signature Algorithm: sha256RSA Not Before: 2014-12-11 04:51:59 p.m. (UTC +8:00) Not After: 2034-12-11 04:51:59 p.m. (UTC +8:00) Thumbprint Algorithm: sha1 Thumbprint: A0:28:DF:21:DB:93:AF:1E:BD:97:0E:0E:68:1C:F9:02:C2:0B:21:85 Thumbprint Algorithm: sha256 Thumbprint: 60:99:30:EB:80:7A:D4:20:AF:DA:2A:8A:A6:1B:67:48:30:39:16:8C:D7:66:E0:99:42:A4:8B:FE:7F:3B:DC:10	Subject Public Key: RSA(2048 bits) Authority Key Identifiers: 1e 0c f7 b6 67 f2 e1 92 26 09 45 c0 55 39 2e 77 3f 42 4a a2 Subject Key Identifiers: cb 83 7d 65 15 af a9 c9 f3 a8 a9 f4 64 7c 79 52 05 74 40 61 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/CRL_SHA2/CA.crl Certificate Policy: [1]1.3.6.1.4.1.23459.100.0.1 [2]1.3.6.1.4.1.23459.100.0.2 [3]1.3.6.1.4.1.23459.100.0.3 [4]2.16.886.1.100.0.1 [5]2.16.886.1.100.0.2 [6]2.16.886.1.100.0.3 [7]2.23.140.1.2.1 [8]2.23.140.1.2.2	■ CA certificate of 2nd Generation of Public Certification Authority signed by eCA. ■ To add the Organization Validation/Domain Validation CP OID adopted by CA/Browser Forum and CP OID with Private Enterprise Number of CHT.
PublicCA - G2	**Intermediate CA Certificate**	
	Subject	Issuer
	OU = Public Certification Authority - G2 O = Chunghwa Telecom Co., Ltd. C = TW	OU = ePKI Root Certification Authority O = Chunghwa Telecom Co., Ltd. C = TW

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

	Certificate related Information	Key Related Information
	Serial Number: 14 35 96 f2 44 1a 71 67 98 3f fc 95 97 41 9b 53 Signature Algorithm: sha256RSA Not Before: 2014-12-11 04:51:59 p.m. (UTC +8:00) Not After : 2034-12-11 04:51:59 p.m. (UTC +8:00) Thumbprint Algorithm: sha1 Thumbprint: 78:62:CA:BA:B6:3A:C7:A7:4E:07:56:A8:F8:6A:2C:02:1A:9F:69:B3 Thumbprint Algorithm: sha256 Thumbprint: DA:E3:43:4F:69:6F:C9:F0:F6:52:E1:B2:A6:F6:9B:5E:92:73:D0:9F:43:BD:3B:DD:47:17:D6:14:1F:8C:D2:C2	Subject Public Key: RSA(2048 bits) Authority Key Identifiers: 1e 0c f7 b6 67 f2 e1 92 26 09 45 c0 55 39 2e 77 3f 42 4a a2 Subject Key Identifiers: cb 83 7d 65 15 af a9 c9 f3 a8 a9 f4 64 7c 79 52 05 74 40 61 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/CRL_SHA2/CA.crl Certificate Policy: [1]1.3.6.1.4.1.23459.100.0.1 [2]1.3.6.1.4.1.23459.100.0.2 [3]1.3.6.1.4.1.23459.100.0.3 [4]2.16.886.1.100.0.1 [5]2.16.886.1.100.0.2 [6]2.16.886.1.100.0.3 [7]2.23.140.1.2.1 [8]2.23.140.1.2.2 [9]2.23.140.1.2.3	■ CA certificate of 2nd Generation of Public Certification Authority signed by eCA. ■ To add CP OID of Individual Validation adopted by CA/Browser Forum.
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

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

	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 : https://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.

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 – 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
PublicCA CPS	1.8	May 28, 2018
PublicCA CPS	1.7	March 21, 2018
PublicCA CPS	1.7(20180214)	February 14, 2018
PublicCA CPS	1.7(20180126)	January 26, 2018
PublicCA CPS	1.7(20171023)	October 23, 2017
PublicCA CPS	1.7(20170714)	July 14, 2017
PublicCA CPS	1.6	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

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

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

Chunghwa Telecom(CHT) provides the following certification authority(CA) services through ePKI Root and Intermediate Certification Authorities listed in Appendix A:

- Subscriber Key Generation Services
- Subscriber Registration
- Certificate Renewal
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Suspension
- Certificate Validation
- Integrated Circuit Card (ICC) Life Cycle Management

The management of CHT is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure, Certification Practice Statement and Certificate Policy for the Chunghwa Telecom eCommerce Public Key Infrastructure(ePKI) on its website, service integrity (including key and certificate life cycle management controls), and CA environmental 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 provide only reasonable assurance with respect to CHT's CA operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

The management of CHT has assessed the controls over its CA operations. Based on that assessment, in CHT Management's opinion, in providing its CA services at Taipei and Taichung, Taiwan during the period from June 1, 2017 through May 31, 2018, CHT has:

- Disclosed its business, key life cycle management, certificate life cycle management, and CA environmental control practices in its certification practice statements and certificate policies listed in Appendix B
- Maintained effective controls to provide reasonable assurance that:
    - The CA's certification practice statement is consistent with its certificate policy; and
    - The CA provides its services in accordance with its certificate policy and certification practice statement
- Maintained effective controls to provide reasonable assurance that:
    - The integrity of keys and certificates it manages was established and protected throughout their life cycles; and
    - Subordinate CA certificate requests are accurate, authenticated and approved
- Maintained effective controls to provide reasonable assurance that:
    - Logical and physical access to CA systems and data was restricted to authorized individuals;
    - The continuity of key and certificate management operations was maintained; and
    - CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity

based on the Trust Service Principles and Criteria for Certification Authorities Version 2.0 including the following:

CA Business Practices Disclosure

- Certification Practice Statement

- Certificate Policy

CA Business Practices Management

- Certificate Policy Management
- Certification Practice Statement Management
- CP and CPS Consistency

CA Environmental Controls

- Security Management
- Asset Classification And Management
- Personnel Security
- Physical And Environmental Security
- Operations Management
- System Access Management
- Systems Development And Maintenance
- Business Continuity Management
- Monitoring And Compliance
- Audit Logging

CA Key Life Cycle Management Controls

- CA Key Generation
- CA Key Storage, Backup And Recovery
- CA Public Key Distribution
- CA Key Usage
- CA Key Archival And Destruction
- CA Key Compromise
- CA Cryptographic Hardware Life Cycle Management

Subscriber Key Life Cycle Management Controls

- Requirements For Subscriber Key Management

Certificate Life Cycle Management Controls

- Subscriber Registration
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution

- Certificate Revocation
- Certificate Validation

Subordinate CA Certificate Life Cycle Management Controls

- Subordinate CA Certificate Life Cycle Management

Signature: Chung, Ming

Title: Principle Engineer

Appendix A – ePKI Root and Intermediate CAs 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 Thumbprint:	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)

	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:A 8:99:78:BD:CD:4F	
	Additional Information	Remark
		■ Self-signed by 2nd Generation of ePKI Root Certification Authority.
eCA cross-signed by eCA – G2	**Self-Issued Certificate**	
	Subject	Issuer
	OU = ePKI Root Certification Authority 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 ca e1 f7 3e fc ac 5b b1 9c 88 c1 c7 2f 6f 7b 2f Signature Algorithm: sha256RSA Not Before: 2015-11-17 04:31:41 p.m. (UTC +8:00) Not After : 2034-12-20 10:31:27 a.m. (UTC +8:00) Thumbprint Algorithm: sha1 Thumbprint: DD:FE:11:1B:8A:9D:C4:76:10:81:19:2F:40: E7:C9:DA:1C:D3:D4:50 Thumbprint Algorithm: sha256 Thumbprint: D1:08:C3:4A:58:C0:E4:A6:16:44:9F:8C:48:3 1:80:23:A2:29:C8:6C:D3:DD:D5:D5:FE:60:4 1:A4:01:C1:6A:14	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
	Certificate Policy: [1]1.3.6.1.4.1.23459.100.0.1 [2]1.3.6.1.4.1.23459.100.0.2 [3]1.3.6.1.4.1.23459.100.0.3 [4]1.3.6.1.4.1.23459.100.0.4 [5]1.3.6.1.4.1.23459.100.0.9 [6]1.3.6.1.4.1.23459.100.0.0 [7]2.16.886.1.100.0.1 [8]2.16.886.1.100.0.2 [9]2.16.886.1.100.0.3 [10]2.16.886.1.100.0.4 [11]2.16.886.1.100.0.0 [12]2.23.140.1.2.1	■ Self-issued certificates are generated to support changes in policy or operations following industry standards such as RFC 5280. ■ This certificate is 1st generation of ePKI Root CA public key with other subject information signed by 2nd generation of ePKI Root CA private key. It is for constructing trust path of 1st generation & 2nd generation of ePKI Root CA key pairs.

	[13]2.23.140.1.2.2 [14]2.23.140.1.2.3 [15]2.23.140.1.1	
eCA - G2 cross-signed by eCA	**Self-Issued Certificate**	
	Subject	Issuer
	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
	Certificate related Information	Key Related Information
	Serial Number: 3b ee e0 91 8e 88 86 ad 46 0f e8 ae 91 0c 9c ba Signature Algorithm: sha256RSA Not Before: 2015-11-17 04:31:41 p.m. (UTC +8:00) Not After : 2034-12-20 10:31:27 a.m. (UTC +8:00) Thumbprint Algorithm: sha1 Thumbprint: C3:CA:F8:57:0C:B1:2D:D0:FC:97:37:BF:CD:0F:08:7C:9B:E6:D2:81 Thumbprint Algorithm: sha256 Thumbprint: 64:71:72:50:AF:8B:02:8D:D8:E5:C0:BA:E4:C9:14:2C:8B:10:35:32:61:2B:C4:87:08:5F:D3:C3:19:F9:C0:67	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
	Additional Information	Remark
	Certificate Policy: [1]1.3.6.1.4.1.23459.100.0.1 [2]1.3.6.1.4.1.23459.100.0.2 [3]1.3.6.1.4.1.23459.100.0.3 [4]1.3.6.1.4.1.23459.100.0.4 [5]1.3.6.1.4.1.23459.100.0.9 [6]1.3.6.1.4.1.23459.100.0.0 [7]2.16.886.1.100.0.1 [8]2.16.886.1.100.0.2 [9]2.16.886.1.100.0.3 [10]2.16.886.1.100.0.4 [11]2.16.886.1.100.0.0 [12]2.23.140.1.2.1 [13]2.23.140.1.2.2 [14]2.23.140.1.2.3 [15]2.23.140.1.1	■ Self-issued certificates are generated to support changes in policy or operations following industry standards such as RFC 5280. ■ This certificate is 2nd generation of ePKI Root CA public key with other subject information signed by 1st generation of ePKI Root CA private key. It is for constructing trust path of 1st generation & 2nd generation of ePKI Root CA key pairs.

<table>
<tr><td rowspan="5">PublicCA</td><td colspan="2">Intermediate CA Certificate</td></tr>
<tr><td>Subject</td><td>Issuer</td></tr>
<tr><td>OU = Public Certification Authority
O = Chunghwa Telecom Co., Ltd.
C = TW</td><td>OU = ePKI Root Certification Authority
O = Chunghwa Telecom Co., Ltd.
C = TW</td></tr>
<tr><td>Certificate related Information</td><td>Key Related Information</td></tr>
<tr><td>Serial Number: 00 c9 53 fe ee b8 95 e9 18 84 ab b2 2a 68 a4 2a 7d
Signature Algorithm: sha1RSA
Not Before: 2007-05-16 06:13:55 p.m. (UTC +8:00)
Not After : 2027-05-16 06:13:55 p.m. (UTC +8:00)
Thumbprint Algorithm: sha1
Thumbprint: 40:FE:0D:8D:9F:99:8A:46:71:F5:C3:26:E5:3F:76:DB:85:59:C2:4F
Thumbprint Algorithm: sha256
Thumbprint: 46:4B:0E:C0:A6:02:F0:19:3D:B5:F3:39:11:88:5A:3A:61:92:1A:D1:6D:26:64:E2:5B:EF:AB:10:CF:A6:ED:25</td><td>Subject Public Key: RSA(2048 bits)
Authority Key Identifiers: 1e 0c f7 b6 67 f2 e1 92 26 09 45 c0 55 39 2e 77 3f 42 4a a2
Subject Key Identifiers: 71 b3 50 31 a0 1b 5b 7b b2 a6 59 7c fd 10 8c 3c ad 3a 3d 7a
Basic Constraint: Subject Type=CA
Path Length Constraint=0
Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)</td></tr>
<tr><td>Additional Information</td><td>Remark</td></tr>
<tr><td>CRL Distribution Point:
http://eca.hinet.net/repository/CRL/CA.crl
Certificate Policy:
[1]2.16.886.1.100.0.1
[2]2.16.886.1.100.0.2
[3]2.16.886.1.100.0.3</td><td>■ CA certificate of 1st Generation of Public Certification Authority signed by eCA.</td></tr>
<tr><td rowspan="3">PublicCA</td><td colspan="2">Intermediate CA Certificate</td></tr>
<tr><td>Subject</td><td>Issuer</td></tr>
<tr><td>OU = Public Certification Authority
O = Chunghwa Telecom Co., Ltd.
C = TW</td><td>OU = ePKI Root Certification Authority
O = Chunghwa Telecom Co., Ltd.
C = TW</td></tr>
</table>

	Certificate related Information	Key Related Information
	Serial Number: 00 97 3c c9 4d 44 cf e9 a2 e1 4f 52 e9 a5 94 a1 5a Signature Algorithm: sha1RSA Not Before: 2007-05-16 06:13:55 p.m. (UTC +8:00) Not After : 2027-05-16 06:13:55 p.m. (UTC +8:00) Thumbprint Algorithm: sha1 Thumbprint: D6:D5:C7:92:AD:6B:2E:3A:B9:B4:23:01:4E:1B:40:E5:76:D8:EC:BF Thumbprint Algorithm: sha1 Thumbprint: 40:FE:0D:8D:9F:99:8A:46:71:F5:C3:26:E5:3F:76:DB:85:59:C2:4F Thumbprint Algorithm: sha256 Thumbprint: 46:4B:0E:C0:A6:02:F0:19:3D:B5:F3:39:11:88:5A:3A:61:92:1A:D1:6D:26:64:E2:5B:EF:AB:10:CF:A6:ED:25	Subject Public Key: RSA(2048 bits) Authority Key Identifiers: 1e 0c f7 b6 67 f2 e1 92 26 09 45 c0 55 39 2e 77 3f 42 4a a2 Subject Key Identifiers: 71 b3 50 31 a0 1b 5b 7b b2 a6 59 7c fd 10 8c 3c ad 3a 3d 7a 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/CRL/CA.crl Certificate Policy: [1]1.3.6.1.4.1.23459.100.0.1 [2]1.3.6.1.4.1.23459.100.0.2 [3]1.3.6.1.4.1.23459.100.0.3 [4]2.16.886.1.100.0.1 [5]2.16.886.1.100.0.2 [6]2.16.886.1.100.0.3 [7]2.23.140.1.2.1 [8]2.23.140.1.2.2	■ CA certificate of 1st Generation of Public Certification Authority signed by eCA. ■ To add the Organization Validation/Domain Validation CP OID adopted by CA/Browser Forum and CP OID with Private Enterprise Number of CHT.
PublicCA - G2	**Intermediate CA Certificate**	
	Subject	Issuer
	OU = Public Certification Authority - G2 O = Chunghwa Telecom Co., Ltd. C = TW	OU = ePKI Root Certification Authority - G2 O = Chunghwa Telecom Co., Ltd. C = TW

	Certificate related Information	Key Related Information
	Serial Number: 00 ce 60 97 fd 33 e1 2d a0 75 ce dc 96 5d c0 c4 a3 Signature Algorithm: sha256RSA Not Before: 2014-12-11 04:51:59 p.m. (UTC +8:00) Not After : 2034-12-11 04:51:59 p.m. (UTC +8:00) Thumbprint Algorithm: sha1 Thumbprint: DD:B1:3C:36:50:3D:BA:D9:4A:B0:B2:E3:89:E3:BB:F4:91:31:3E:5F Thumbprint Algorithm: sha256 Thumbprint: F5:FB:67:C8:45:3E:DA:34:DB:EC:8A:76:65:74:F0:7A:03:54:8C:08:4A:F2:F5:E6:45:5E:A7:69:60:8D:9A:D5	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: cb 83 7d 65 15 af a9 c9 f3 a8 a9 f4 64 7c 79 52 05 74 40 61 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]1.3.6.1.4.1.23459.100.0.1 [2]1.3.6.1.4.1.23459.100.0.2 [3]1.3.6.1.4.1.23459.100.0.3 [4]1.3.6.1.4.1.23459.100.0.9 [5]2.16.886.1.100.0.1 [6]2.16.886.1.100.0.2 [7]2.16.886.1.100.0.3 [8]2.23.140.1.2.1 [9]2.23.140.1.2.2 [10]2.23.140.1.2.3	■ CA certificate of 2nd Generation of Public Certification Authority signed by ePKI Root Certification Authority - G2. ■ Add 1.3.6.1.4.1.23459.100.0.9 CP OID in Certificate Policy extension for PDF Signing. ■ CA certificate was published in the repository : http://eca.hinet.net/en/repository_c2.htm#PublicCA_CA2 ■ News of the publication of CA certificate was announced on 2016/10/13 : http://eca.hinet.net/en/index.htm , then moved to : https://eca.hinet.net/en/history.htm
PublicCA - G2	**Intermediate CA Certificate**	
	Subject	Issuer
	OU = Public Certification Authority - G2 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: 00 c4 23 d2 21 91 86 8f ac 4e e2 fc e4 a0 11 d1 a7 Signature Algorithm: sha256RSA Not Before: 2014-12-11 04:51:59 p.m. (UTC +8:00) Not After: 2034-12-11 04:51:59 p.m. (UTC +8:00) Thumbprint Algorithm: sha1 Thumbprint: A0:28:DF:21:DB:93:AF:1E:BD:97:0E:0E:68:1C:F9:02:C2:0B:21:85 Thumbprint Algorithm: sha256 Thumbprint: 60:99:30:EB:80:7A:D4:20:AF:DA:2A:8A:A6:1B:67:48:30:39:16:8C:D7:66:E0:99:42:A4:8B:FE:7F:3B:DC:10	Subject Public Key: RSA(2048 bits) Authority Key Identifiers: 1e 0c f7 b6 67 f2 e1 92 26 09 45 c0 55 39 2e 77 3f 42 4a a2 Subject Key Identifiers: cb 83 7d 65 15 af a9 c9 f3 a8 a9 f4 64 7c 79 52 05 74 40 61 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/CRL_SHA2/CA.crl Certificate Policy: [1]1.3.6.1.4.1.23459.100.0.1 [2]1.3.6.1.4.1.23459.100.0.2 [3]1.3.6.1.4.1.23459.100.0.3 [4]2.16.886.1.100.0.1 [5]2.16.886.1.100.0.2 [6]2.16.886.1.100.0.3 [7]2.23.140.1.2.1 [8]2.23.140.1.2.2	■ CA certificate of 2nd Generation of Public Certification Authority signed by eCA. ■ To add the Organization Validation/Domain Validation CP OID adopted by CA/Browser Forum and CP OID with Private Enterprise Number of CHT.
PublicCA - G2	**Intermediate CA Certificate**	
	Subject	Issuer
	OU = Public Certification Authority - G2 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: 14 35 96 f2 44 1a 71 67 98 3f fc 95 97 41 9b 53 Signature Algorithm: sha256RSA Not Before: 2014-12-11 04:51:59 p.m. (UTC +8:00) Not After : 2034-12-11 04:51:59 p.m. (UTC +8:00) Thumbprint Algorithm: sha1 Thumbprint: 78:62:CA:BA:B6:3A:C7:A7:4E:07:56:A8:F8:6A:2C:02:1A:9F:69:B3 Thumbprint Algorithm: sha256 Thumbprint: DA:E3:43:4F:69:6F:C9:F0:F6:52:E1:B2:A6:F6:9B:5E:92:73:D0:9F:43:BD:3B:DD:47:17:D6:14:1F:8C:D2:C2	Subject Public Key: RSA(2048 bits) Authority Key Identifiers: 1e 0c f7 b6 67 f2 e1 92 26 09 45 c0 55 39 2e 77 3f 42 4a a2 Subject Key Identifiers: cb 83 7d 65 15 af a9 c9 f3 a8 a9 f4 64 7c 79 52 05 74 40 61 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/CRL_SHA2/CA.crl Certificate Policy: [1]1.3.6.1.4.1.23459.100.0.1 [2]1.3.6.1.4.1.23459.100.0.2 [3]1.3.6.1.4.1.23459.100.0.3 [4]2.16.886.1.100.0.1 [5]2.16.886.1.100.0.2 [6]2.16.886.1.100.0.3 [7]2.23.140.1.2.1 [8]2.23.140.1.2.2 [9]2.23.140.1.2.3	■ CA certificate of 2nd Generation of Public Certification Authority signed by eCA. ■ To add CP OID of Individual Validation adopted by CA/Browser Forum.
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 : https://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
PublicCA CPS	1.8	May 28, 2018
PublicCA CPS	1.7	March 21, 2018
PublicCA CPS	1.7(20180214)	February 14, 2018
PublicCA CPS	1.7(20180126)	January 26, 2018
PublicCA CPS	1.7(20171023)	October 23, 2017
PublicCA CPS	1.7(20170714)	July 14, 2017
PublicCA CPS	1.6	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