



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 SSL certification authority(CA) services at Taipei and Taichung, Taiwan, 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 Certificate practices and its commitment to provide SSL Certificates in conformity with the applicable CA/Browser Forum Guidelines in its certification practice statements and certificate policies listed in Appendix B
- Maintained effective controls to provide reasonable assurance that:
 - The Certificate Policies and/or Certificate Practice Statements are available on a 24x7 basis and updated annually;
 - Subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified;
 - The integrity of keys and certificates it manages was established and protected throughout their life cycles;
 - 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



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

 CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity

• Maintained effective controls to meet the Network and Certificate System Security Requirements set forth by the CA/Browser Forum

based on the WebTrust for Certification Authorities – SSL Baseline with Network Security – Version 2.2.

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 (1) obtaining an understanding of CHT's key and SSL certificate life cycle management business practices and its controls over key and SSL certificate integrity, over the continuity of key and certificate life cycle management operations, and over the development, maintenance, and operation of systems integrity; (2) testing transactions executed in accordance with disclosed key and certificate life cycle management business practices; (3) testing and evaluating the operating effectiveness of the controls; and (4) performing such other procedures as we considered necessary in the circumstances.

We believe that our examination provides a reasonable basis for our opinion.

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.





Taipei City 110, Taiwan, R.O.C.

Tel: +886 2 2346 6168 Fax: +886 2 2346 6068

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.

In our opinion, for the period from June 1, 2017 through May 31, 2018, CHT management's assertion, as set forth, is fairly stated, in all material respects, based on the WebTrust for Certification Authorities – SSL Baseline with Network Security – Version 2.2.

This report does not include any representation as to the quality of the CHT services beyond those covered by the WebTrust for Certification Authorities – SSL Baseline with Network Security – Version 2.2, or the suitability of any of CHT's services for any customer's intended purpose.

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

July 9, 2018

DIK TUTERNATZONAL





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

	Root CA Certificate		
	Subject OU = ePKI Root Certification Authority O = Chunghwa Telecom Co., Ltd. C = TW	Issuer OU = ePKI Root Certification Authority O = Chunghwa Telecom Co., Ltd. C = TW	
eCA	Certificate 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:F4:56:4 B:CF:E2:3D:69:C6:F0 Thumbprint Algorithm: sha256 C0:A6:F4:DC:63:A2:4B:FD:CF:54:EF:2A:6 A:08:2A:0A:72:DE:35:80:3E:2F:F5:FF:52:7 A:E5:D8:72:06:DF:D5	Key Related Information 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 1 st Generation of ePKI Root Certification Authority.	
	Root CA Certificate		
	Subject CN = ePKI Root Certification Authority - G2 O = Chunghwa Telecom Co., Ltd. C = TW	Issuer CN = ePKI Root Certification Authority - G2 O = Chunghwa Telecom Co., Ltd. C = TW	
eCA - G2	Certificate 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	Key Related Information 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:A 8:99:78:BD:CD:4F Additional Information	Remark ■ Self-signed by 2 nd Generation of ePKI Root Certification Authority.
	Self-Issue	d Certificate
	Subject OU = ePKI Root Certification Authority O = Chunghwa Telecom Co., Ltd. C = TW	Issuer CN = ePKI Root Certification Authority - G2 O = Chunghwa Telecom Co., Ltd. C = TW
eCA cross- signed by eCA – G2	Certificate 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	Key Related Information 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 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	Remark ■ 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





	[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.
	Self-Issu	ied Certificate
	Subject CN = ePKI Root Certification Authority - G2 O = Chunghwa Telecom Co., Ltd. C = TW	Issuer OU = ePKI Root Certification Authority O = Chunghwa Telecom Co., Ltd. C = TW
	Certificate related Information Serial Number: 3b ee e0 91 8e 88 86 ad 46 0f e8 ae 91 0c 9c ba	Key Related Information Subject Public Key: RSA(4096 bits) Subject Key Identifiers: 72 5b ba aa 72 38 ee 25
eCA - G2 cross- signed by eCA	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:	90 24 b5 94 22 fa 09 88 ca 8b 0a fb
	C9:14:2C:8B:10:35:32:61:2B:C4:87:08:5F:D 3:C3:19:F9:C0:67	
	Additional Information 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	 Remark 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.



	[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 Intermediate Subject OU = Public Certification Authority O = Chunghwa Telecom Co., Ltd. C = TW	CA Certificate Issuer OU = ePKI Root Certification Authority O = Chunghwa Telecom Co., Ltd. C = TW
PublicCA	Certificate 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:E5:3 F:76:DB:85:59:C2:4F Thumbprint Algorithm: sha256 Thumbprint: 46:4B:0E:C0:A6:02:F0:19:3D:B5:F3:39:11:8 8:5A:3A:61:92:1A:D1:6D:26:64:E2:5B:EF:A B:10:CF:A6:ED:25	Key Related Information 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 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	Remark CA certificate of 1 st Generation of Public Certification Authority signed by eCA.
PublicC A	Subject	CA Certificate Issuer
Tuoneca	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., Sinvi District.

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

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



	Certificate related Information	Key Related Information
	Serial Number: 00 ce 60 97 fd 33 e1 2d a0 75	Subject Public Key: RSA(2048 bits)
	ce dc 96 5d c0 c4 a3	Authority Key Identifiers: 72 5b ba aa 72 38 ee
	Signature Algorithm: sha256RSA	25 90 24 b5 94 22 fa 09 88 ca 8b 0a fb
	Not Before: 2014-12-11 04:51:59 p.m. (UTC	Subject Key Identifiers: cb 83 7d 65 15 af a9 c9
	+8:00)	f3 a8 a9 f4 64 7c 79 52 05 74 40 61
	Not After: 2034-12-11 04:51:59 p.m. (UTC	Basic Constraint: Subject Type=CA
	+8:00)	Path Length Constraint=0
	l /	
	Thumbprint Algorithm: sha1	Key Usage: Certificate Signing, Off-line CRL
	Thumbprint:	Signing, CRL Signing (06)
	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:A	
	7:69:60:8D:9A:D5	
	Additional Information	Remark
	CRL Distribution Point:	■ CA certificate of 2 nd Generation of Public
	http://eca.hinet.net/repository/CRL2/CA.crl	Certification Authority signed by
	Certificate Policy:	ePKI Root Certification Authority - G2.
	[1]1.3.6.1.4.1.23459.100.0.1	Add 1.3.6.1.4.1.23459.100.0.9 CP OID in
	[2]1.3.6.1.4.1.23459.100.0.2	
		Certificate Policy extension for PDF
	[3]1.3.6.1.4.1.23459.100.0.3	Signing.
	[4]1.3.6.1.4.1.23459.100.0.9	CA certificate was published in the
	[5]2.16.886.1.100.0.1	repository:
	[6]2.16.886.1.100.0.2	http://eca.hinet.net/en/repository_c2.htm#
	[7]2.16.886.1.100.0.3	PublicCA_CA2
	[8]2.23.140.1.2.1	■ News of the publication of CA certificate
	[9]2.23.140.1.2.2	was announced on 2016/10/13:
	[10]2.23.140.1.2.3	http://eca.hinet.net/en/index.htm,
		then moved to :
		https://eca.hinet.net/en/history.htm
	Intoumodia	te CA Certificate
	Intermedia	THE CA CEI UIICALE
	Subject	Issuer
	OU = Public Certification Authority - G2	OU = ePKI Root Certification Authority
Dulatia CA	O = Chunghwa Telecom Co., Ltd.	O = Chunghwa Telecom Co., Ltd.
PublicCA	C = TW	C = TW
- G2		
<u> </u>		



	Certificate related Information	 Key Related Information
	Certificate 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:A4:8 B:FE:7F:3B:DC:10	Key Related Information 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 CRL Distribution Point: http://eca.hinet.net/repository/CRL_SHA2/C A.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	 Remark ■ 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.
	Intermediate CA Certificate	
PublicCA - G2	O = Chunghwa Telecom Co., Ltd.	Issuer OU = ePKI Root Certification Authority O = Chunghwa Telecom Co., Ltd. C = TW



Scrial Number: 14 35 96 12 44 1a 71 67 98 3f for 95 97 41 9b 53		Certificate related Information	Key Related Information
Repair	ļ		
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 Algorithm: sha1 Thumbprint Algorithm: sha256 Thumbprint Algorithm: sha256 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 Additional Information CRL Distribution Point: http://eea.hinet.net/repository/CRL_SHA2/CA.crl Certificate Policy: [1]13.6.1.4.1.23459.100.0.1 [2]1.3.6.1.4.1.23459.100.0.2 [6]2.16.886.1.100.0.2 [6]2.16.886.1.100.0.2 [6]2.23.140.1.2.1 [8]2.23.140.1.2.1 [8]2.23.140.1.2.2 [9]2.23.140.1.2.3 Intermediate CA Certificate Subject CN = cPKI EV SSL Certification Authority - G2 O = Chunghwa Telecom Co., Ltd. C = TW CTW Car TW Car TW Car TW Car			l • · · · · · · · · · · · · · · · · · ·
+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: DA:E3:43:4F:69:6F:C9:F0:F6:52:E1:B2:A6:F 6:9B:5E:92:73:D0:9F:43:BD:3B:DD:47:17:D 6:14:1F:8C:D2:C2 Additional Information CRL Distribution Point: http://eca.hinet.net/repository/CRL_SHA2/C A.crl Certificate Policy: [1]1.3.6.1.4.1.23459.100.0.1 [2]1.3.6.1.4.1.23459.100.0.3 [4]2.16.886.1.100.0.2 [6]2.16.886.1.100.0.2 [6]2.16.886.1.100.0.3 [7]2.23.140.1.2.1 [8]2.23.140.1.2.3 Intermediate CA Certificate Subject CN = ePK1 EV SSL Certification Authority - G2 O = Chunghwa Telecom Co., Ltd. C = TW Signing (06) Rey Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06) Rey Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06) Rey Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06) Rey Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06) Rey Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06) Rey Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06) Rey Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06) Rey Usage: Certificate Signing, Off-line CRL Si		, .	
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: DA:E3:43:4F:69:6F:C9:F0:F6:52:E1:B2:A6:F 6:9B:5E:92:73:D0:9F:43:BD:3B:DD:47:17:D 6:14:1F:8C:D2:C2 Additional Information CRL Distribution Point: http://eca.hinet.net/repository/CRL_SHA2/C A.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]2.16.886.1.100.0.2 [6]2.16.886.1.100.0.2 [6]2.16.886.1.100.0.3 [7]2.23.140.1.2.3 Intermediate CA Certificate Subject CN = ePKI EV SSL Certification Authority - G1 CPKI EV SSL CN = ePKI Root Certification Authority - G2 O = Chunghwa Telecom Co., Ltd. C		* `	"
+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 DA:E3:43:4F:69:6F:C9:F0:F6:52:E1:B2:A6:F 6:9B:5E:92:73:D0:9F:43:BD:3B:DD:47:17:D 6:14:1F:8C:D2:C2 Additional Information CRL Distribution Point: http://eca.hinet.net/repository/CRL_SHA2/C A.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]2.16.886.1.100.0.2 [6]2.16.886.1.100.0.3 [7]2.23.140.1.2.1 [8]2.23.140.1.2.3 Intermediate CA Certificate Subject CN = ePKI EV SSL Certification Authority - G2 O = Chunghwa Telecom Co., Ltd. C = TW Path Length Constraint=0 Rey Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06) Rey Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06) Rey Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06) Rey Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06) Rey Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06) Rey Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06) Rey Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06) Rey Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06) Rey Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06) Rey Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06) Rey Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06) Remark CA certificate of 2 nd Generation of Public Certification of Public Certification Authority signed by cA. To add CP OID of Individual Validation adopted by CA/Browser Forum. Intermediate CA Certificate of 2 nd Generation of Public Certification Authority of Signing (06) CRL Distribution of Oil Authority of Signing (06) Remark CA certificate of 2 nd Generation of Public Certification Authority of Signing (06) Certificate of 2 nd Generation of Public Certification Authority of Signing (06) Remark CA certificate of 2 nd Generation of Public Certification Authority of Signing (06) Cer			
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:F 6:9B:5E:92:73:D0:9F:43:BD:3B:DD:47:17:D 6:14:1F:8C:D2:C2 Additional Information CRL Distribution Point: http://eca.hinet.net/repository/CRL_SHA2/C A.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]2.16.886.1.100.0.2 [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 Intermediate CA Certificate Subject CN = ePKI EV SSL Certification Authority - G2 G1 O = Chunghwa Telecom Co., Ltd. C = TW Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06) Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06) Signing, CRL Signing (06) Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06) Signing, CRL Signing (06) **CA Certificate of 2 nd Generation of Public Certification Authority signed by eCA. To add CP OID of Individual Validation adopted by CA/Browser Forum.		· ` `	
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:F 6:9B:5E:92:73:D0:9F:43:BD:3B:DD:47:17:D 6:14:1F:8C:D2:C2 Additional Information CRL Distribution Point: http://eca.hinet.net/repository/CRL_SHA2/C A.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]2.16.886.1.100.0.3 [7]2.23.140.1.2.1 [8]2.23.140.1.2.2 [9]2.23.140.1.2.3 Intermediate CA Certificate Subject CN = ePKI EV SSL Certification Authority - G2 G1 O = Chunghwa Telecom Co., Ltd. C = TW Signing, CRL Signing (06) Signing, CRL Signing (16) Signing, CR L Signing (16) Signing, CRL Signing (l /	
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:B3:43:4F:69:6F:C9:F0:F6:52:E1:B2:A6:F 6:9B:5E:92:73:D0:9F:43:BD:3B:DD:47:17:D 6:14:1F:8C:D2:C2 Additional Information CRL Distribution Point: http://eca.hinet.net/repository/CRL_SHA2/C A.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]2.16.886.1.100.0.2 [6]2.16.886.1.100.0.2 [6]2.16.886.1.100.0.2 [6]2.12.3.140.1.2.1 [8]2.23.140.1.2.2 [9]2.23.140.1.2.3 Intermediate CA Certificate Subject CN = ePKI EV SSL Certification Authority - G2 O = Chunghwa Telecom Co., Ltd. C = TW			1 2 5
6A:2C:02:1A:9F:69:B3 Thumbprint Algorithm: sha256 Thumbprint: DA:E3:43:4F:69:6F:C9:F0:F6:52:E1:B2:A6:F 6:9B:5E:92:73:D0:9F:43:BD:3B:DD:47:17:D 6:14:1F:8C:D2:C2 Additional Information CRL Distribution Point: http://eca.hinet.net/repository/CRL_SHA2/C A.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]13.6.1.4.1.23459.100.0.3 [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 Intermediate CA Certificate Subject CN = ePKI EV SSL Certification Authority - G1 O = Chunghwa Telecom Co., Ltd. C = TW			Signing, CKL Signing (00)
Thumbprint Algorithm: sha256 Thumbprint: DA:E3:43:4F:69:6F:C9:F0:F6:52:E1:B2:A6:F 6:98:5E:92:73:D0:9F:43:BD:3B:DD:47:17:D 6:14:1F:8C:D2:C2 Additional Information CRL Distribution Point: http://eca.hinet.net/repository/CRL_SHA2/C A.crl Certificate Policy: [1]1.3.6.1.4.1.23459.100.0.1 [2]11.3.6.1.4.1.23459.100.0.2 [3]31.3.6.1.4.1.23459.100.0.3 [4]2.16.886.1.100.0.2 [6]2.16.886.1.100.0.2 [6]2.16.886.1.100.0.2 [6]2.16.886.1.100.0.2 [8]2.23.140.1.2.1 [8]2.23.140.1.2.2 [9]2.23.140.1.2.3 Intermediate CA Certificate Subject CN = ePKI EV SSL Certification Authority - G1 G1 O = Chunghwa Telecom Co., Ltd. C = TW			
Thumbprint:			
DA:E3:43:4F:69:6F:C9:F0:F6:52:E1:B2:A6:F 6:9B:5E:92:73:D0:9F:43:BD:3B:DD:47:17:D 6:14:1F:8C:D2:C2 Additional Information CRL Distribution Point:			
Additional Information			
Additional Information CRL Distribution Point: http://eca.hinet.net/repository/CRL_SHA2/C A.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 Intermediate CA Certificate Subject CN = ePKI EV SSL Certification Authority - G1 O = Chunghwa Telecom Co., Ltd. Ca certificate of 2 nd Generation of Public Certification Authority signed by cA. To add CP OID of Individual Validation adopted by CA/Browser Forum. Intermediate by CA/Browser Forum. Intermediate CA Certificate Subject Subject Subject Subject Subject Subject CN = ePKI Root Certification Authority - G2 O = Chunghwa Telecom Co., Ltd. C = TW		6:9B:5E:92:73:D0:9F:43:BD:3B:DD:47:17:D	
CRL Distribution Point: http://eca.hinet.net/repository/CRL_SHA2/C A.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 Intermediate CA Certificate Subject CN = ePKI EV SSL Certification Authority - G2 O = Chunghwa Telecom Co., Ltd. CA certificate of 2 nd Generation of Public Certification Authority signed by eCA. To add CP OID of Individual Validation adopted by CA/Browser Forum.		6:14:1F:8C:D2:C2	
http://eca.hinet.net/repository/CRL_SHA2/C A.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 Intermediate CA Certificate Subject CN = ePKI EV SSL Certification Authority - G2 G1 O = Chunghwa Telecom Co., Ltd. Certification Authority signed by eCA. To add CP OID of Individual Validation adopted by CA/Browser Forum. Intermediate by CA/Browser Forum. To add CP OID of Individual Validation adopted by CA/Browser Forum. Intermediate by CA/Browser Forum. Intermediate CA Certificate Subject CN = ePKI Root Certification Authority - G2 O = Chunghwa Telecom Co., Ltd. C = TW		Additional Information	Remark
A.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 Intermediate CA Certificate Subject CN = ePKI EV SSL Certification Authority - G2 G1 O = Chunghwa Telecom Co., Ltd. C = TW	•	CRL Distribution Point:	■ CA certificate of 2 nd Generation of Public
Certificate Policy: adopted by CA/Browser Forum. [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 Intermediate CA Certificate Subject		http://eca.hinet.net/repository/CRL_SHA2/C	
[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 Intermediate CA Certificate Subject CN = ePKI EV SSL Certification Authority - GN = ePKI Root Certification Authority - G2 G1 O = Chunghwa Telecom Co., Ltd. C = TW			
[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 Intermediate CA Certificate Subject CN = ePKI EV SSL Certification Authority - CN = ePKI Root Certification Authority - G2 G1 O = Chunghwa Telecom Co., Ltd. C = TW	l	l	adopted by CA/Browser Forum.
[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 Intermediate CA Certificate Subject CN = ePKI EV SSL Certification Authority - CN = ePKI Root Certification Authority - G2 ePKI G1 O = Chunghwa Telecom Co., Ltd. C = TW	l		
[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 Intermediate CA Certificate Subject Issuer CN = ePKI EV SSL Certification Authority - CN = ePKI Root Certification Authority - G2 ePKI G1 O = Chunghwa Telecom Co., Ltd. EV SSL O = Chunghwa Telecom Co., Ltd. C = TW	l		
[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 Intermediate CA Certificate Subject Issuer CN = ePKI EV SSL Certification Authority - CN = ePKI Root Certification Authority - G2 O = Chunghwa Telecom Co., Ltd. C = TW	l		
[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 Intermediate CA Certificate Subject CN = ePKI EV SSL Certification Authority - G2 ePKI G1 G1 O = Chunghwa Telecom Co., Ltd. C = TW			
$[7]2.23.140.1.2.1 \\ [8]2.23.140.1.2.2 \\ [9]2.23.140.1.2.3$ $[9]2$			
[8]2.23.140.1.2.2 [9]2.23.140.1.2.3 Intermediate CA Certificate Subject CN = ePKI EV SSL Certification Authority - CN = ePKI Root Certification Authority - G2 ePKI G1 O = Chunghwa Telecom Co., Ltd. C = TW			
		- -	
Intermediate CA Certificate Subject Issuer CN = ePKI EV SSL Certification Authority - CN = ePKI Root Certification Authority - G2 ePKI G1 O = Chunghwa Telecom Co., Ltd. EV SSL O = Chunghwa Telecom Co., Ltd. C = TW			
Subject Issuer CN = ePKI EV SSL Certification Authority - CN = ePKI Root Certification Authority - G2 ePKI G1 O = Chunghwa Telecom Co., Ltd. C = TW			
ePKI EV SSL Certification Authority - CN = ePKI Root Certification Authority - G2 ePKI G1 O = Chunghwa Telecom Co., Ltd. EV SSL O = Chunghwa Telecom Co., Ltd. C = TW		Intermediate	CA Certificate
ePKI EV SSL Certification Authority - CN = ePKI Root Certification Authority - G2 ePKI G1 O = Chunghwa Telecom Co., Ltd. EV SSL O = Chunghwa Telecom Co., Ltd.		Subject	Issuer
ePKI G1 O = Chunghwa Telecom Co., Ltd. C = TW		3	
θ		G1	•
CA $C = TW$		_	C = TW
	CA	C = TW	



Certificate related Information Serial Number: 00 f7 4e 18 0c 99 e2 7b 8d 9f 79 4f b1 b7 c0 bf 48	Key Related Information Subject Public Key: RSA(2048 bits) Authority Key Identifiers: 72 5b ba aa 72 38 ee
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 1DB:1A:29:4B:F6:D8:1F:82:D9:B4:E7:1F:50:2F:0B:15:A1:FC:08	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 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.





9F.-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., Sinvi District.

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



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 SSL Certification Authority(CA) services located at Taipei and Taichung, Taiwan. Based on that assessment, in CHT Management's opinion, in providing its SSL CA services at Taipei and Taichung, Taiwan, 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 Certificate practices and its commitment to provide SSL Certificates in conformity with the applicable CA/Browser Forum Guidelines in its certification practice statements and certificate policies listed in Appendix B
- Maintained effective controls to provide reasonable assurance that:
 - The Certificate Policies and/or Certificate Practice Statements are available on a 24x7 basis and updated annually;
 - Subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified;
 - The integrity of keys and certificates it manages was established and protected throughout their life cycles;
 - 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

() 中華電信

Page 2

 Maintained effective controls to meet the Network and Certificate System Security Requirements set forth by the CA/Browser Forum.

in accordance with the WebTrust for Certification Authorities – SSL Baseline with Network Security – Version 2.2.

Signature:

Chung, Ming

Title:

Principle Engineer



Appendix A – ePKI Root and Intermediate CAs within the Audit Report Scope

	Root CA Certificate		
	Subject	Issuer	
	OU = ePKI Root Certification Authority	OU = ePKI Root Certification Authority	
	O = Chunghwa Telecom Co., Ltd. C = TW	O = Chunghwa Telecom Co., Ltd. C = TW	
	C - 1 W	C - I W	
	Certificate Related Information	Key Related Information	
	Serial Number: 15 c8 bd 65 47 5c af b8 97 00	Subject Public Key: RSA(4096 bits)	
	5e e4 06 d2 bc 9d	Subject Key Identifiers: 1e 0c f7 b6 67 f2 e1 92	
	Signature Algorithm: sha1RSA	26 09 45 c0 55 39 2e 77 3f 42 4a a2	
	Not Before: 2004-12-20 10:31:27 a.m. (UTC		
eCA	+8:00)		
COL	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:F4:56:4		
	B:CF:E2:3D:69:C6:F0		
	Thumbprint Algorithm: sha256		
	C0:A6:F4:DC:63:A2:4B:FD:CF:54:EF:2A:6		
	A:08:2A:0A:72:DE:35:80:3E:2F:F5:FF:52:7		
	A:E5:D8:72:06:DF:D5		
	Additional Information	Remark	
		Self-signed by 1st Generation of ePKI Root	
		Certification Authority.	
	Root CA	Certificate	
	Subject	Issuer	
	CN = ePKI Root Certification Authority - G2	CN = ePKI Root Certification Authority - G2	
	O = Chunghwa Telecom Co., Ltd.	O = Chunghwa Telecom Co., Ltd.	
	C = TW	C = TW	
	Certificate Related Information	Key Related Information	
	Serial Number: 00 d6 96 2e c1 0a 15 93 12 af	•	
eCA - G2	8f 63 bc d4 44 c9 5b	Subject Key Identifiers: 72 5b ba aa 72 38 ee 25	
	Signature Algorithm: sha256RSA	90 24 b5 94 22 fa 09 88 ca 8b 0a fb	
	Not Before: 2015-11-17 04:23:42 p.m. (UTC	Key Usage: Certificate Signing, Off-line CRL	
	+8:00)	Signing, CRL Signing (06)	
	Not After: 2037-12-31 11:59:59 p.m. (UTC +8:00)		
	Thumbprint Algorithm: sha1		
	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:A 8:99:78:BD:CD:4F Additional Information	Remark
	Self-signed by 2 nd Generation of ePKI Root Certification Authority.
Self-Issued	d 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 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	 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.



	[15]2.23.140.1.1	
	Self-Issa	ued 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
eCA - G2 cross-	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:D	Subject Public Key: RSA(4096 bits) Subject Key Identifiers: 72 5b ba aa 72 38 ee 2 90 24 b5 94 22 fa 09 88 ca 8b 0a fb
signed by eCA		
	Additional Information 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 operation following industry standards such as RF 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.



	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 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:	Key Related Information 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)	
PublicCA	40:FE:0D:8D:9F:99:8A:46:71:F5:C3:26:E5:3 F:76:DB:85:59:C2:4F Thumbprint Algorithm: sha256 Thumbprint: 46:4B:0E:C0:A6:02:F0:19:3D:B5:F3:39:11:8 8:5A:3A:61:92:1A:D1:6D:26:64:E2:5B:EF:A B:10:CF:A6:ED:25		
	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 1 st Generation of Public Certification Authority signed by eCA.	



-	Intermediate	CA Certificate	
· -	J	Issuer	
	O = Chunghwa Telecom Co., Ltd.	OU = ePKI Root Certification Authority O = Chunghwa Telecom Co., Ltd. C = TW	
PublicCA + 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	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	Key Related Information 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)	



	7	I
	Additional Information 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	Remark CA certificate of 1 st 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.
	Intermediate	CA Certificate
	Subject 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
PublicCA - G2	Certificate 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	



	_]	
	Additional Information	Remark
	CRL Distribution Point:	■ CA certificate of 2 nd Generation of Public
	http://eca.hinet.net/repository/CRL2/CA.crl	Certification Authority signed by
	Certificate Policy:	ePKI Root Certification Authority - G2.
	[1]1.3.6.1.4.1.23459.100.0.1	Add 1.3.6.1.4.1.23459.100.0.9 CP OID in
	[2]1.3.6.1.4.1.23459.100.0.2	Certificate Policy extension for PDF
	[3]1.3.6.1.4.1.23459.100.0.3	Signing.
		_ ~ ~
	[4]1.3.6.1.4.1.23459.100.0.9	1
	[5]2.16.886.1.100.0.1	repository:
	[6]2.16.886.1.100.0.2	http://eca.hinet.net/en/repository_c2.htm#
	[7]2.16.886.1.100.0.3	PublicCA_CA2
	[8]2.23.140.1.2.1	■ News of the publication of CA certificate
	[9]2.23.140.1.2.2	was announced on 2016/10/13:
	[10]2.23.140.1.2.3	http://eca.hinet.net/en/index.htm,
		then moved to:
		https://eca.hinet.net/en/history.htm
	T	<u> </u>
}	Intermedia	nte CA Certificate
	Subject	Issuer
	OU = Public Certification Authority - G2	OU = ePKI Root Certification Authority
	O = Chunghwa Telecom Co., Ltd.	O = Chunghwa Telecom Co., Ltd.
	C = TW	C = TW
	Certificate related Information	Key Related Information
PublicCA		·
- G2		Subject Public Key: RSA(2048 bits)
	e2 fc e4 a0 11 d1 a7	Authority Key Identifiers: 1e 0c f7 b6 67 f2 e1
	Signature Algorithm: sha256RSA	92 26 09 45 c0 55 39 2e 77 3f 42 4a a2
	Not Before: 2014-12-11 04:51:59 p.m. (UTC	Subject Key Identifiers: cb 83 7d 65 15 af a9 c9
	+8:00)	f3 a8 a9 f4 64 7c 79 52 05 74 40 61
	Not After: 2034-12-11 04:51:59 p.m. (UTC	Basic Constraint: Subject Type=CA
	+8:00)	Path Length Constraint=0
	Thumbprint Algorithm: sha1	Key Usage: Certificate Signing, Off-line CRL
	Thumbprint:	Signing, CRL Signing (06)
	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:A4:8	
	B:FE:7F:3B:DC:10	
	D.T.E. / F.3D.DC.10	



	1	
	Additional Information CRL Distribution Point: http://eca.hinet.net/repository/CRL_SHA2/C A.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	Remark CA certificate of 2 nd 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.
	Intermediate	CA Certificate
	Subject	Iccuar
	Subject OU = Public Certification Authority - G2 O = Chunghwa Telecom Co., Ltd. C = TW	Issuer OU = ePKI Root Certification Authority O = Chunghwa Telecom Co., Ltd. C = TW
PublicCA	Certificate related Information	Key Related Information
- G2	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)



	1	L .
	Additional Information CRL Distribution Point: http://eca.hinet.net/repository/CRL_SHA2/C A.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	Remark ■ CA certificate of 2 nd Generation of Public Certification Authority signed by eCA. ■ To add CP OID of Individual Validation adopted by CA/Browser Forum.
	Intermediate	CA Certificate
	Subject CN = ePKI EV SSL Certification Authority - G1 O = Chunghwa Telecom Co., Ltd. C = TW	Issuer CN = ePKI Root Certification Authority - G2 O = Chunghwa Telecom Co., Ltd. C = TW
ePKI EV SSL CA	Certificate 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	



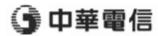
Additional Information	Remark
CRL Distribution Point:	■ CA certificate of ePKI EV SSL
http://eca.hinet.net/repository/CRL2/CA.crl	
Certificate Policy:	eCA - G2 on 2016-02-04.
[1]2.23.140.1.1	■ CA certificate was published in the
	repository:
	http://eca.hinet.net/en/repository c2.htm
	News of the publication 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.
	accomplished on December 21, 2010.



Page 13

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



Page 14

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