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

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

INDEPENDENT ASSURANCE REPORT

To the management of Chunghwa Telecom(CHT):

We have been engaged, in a reasonable assurance engagement, to report on CHT management's assertion that for its Certification Authority (CA) operations at Taipei and Taichung, Taiwan, as of 22 February 2019 for its CAs as enumerated in Appendix A, CHT has:

- disclosed its SSL certificate lifecycle management business practices in its:
  - HiPKI EV TLS CA Certification Practice Statement Version 1.0;
  - HiPKI Root Certification Authority Certification Practice Statement Version 1.0; and
  - HiPKI Certificate Policy Version 1.0

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

- suitably designed, and placed into operation, controls to provide reasonable assurance that:
  - the integrity of keys and SSL certificates it manages is established and protected throughout their lifecycles; and
  - SSL subscriber information is properly authenticated (for the registration activities performed by CHT)

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

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

And, for its CAs as enumerated in Attachment A:

- suitably designed, and placed into operation, controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3.

Certification authority's responsibilities

CHT's management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3.

Our independence and quality control

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

The firm applies International Standard on Quality Control 1, and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

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

Auditor's responsibilities

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

(1) obtaining an understanding of CHT's key and certificate lifecycle management business practices and its controls over key and certificate integrity, over the authenticity and confidentiality of subscriber and relying party information, over the continuity of key and certificate lifecycle management operations and over development, maintenance and operation of systems integrity;

(2) evaluating the suitability of the design of the controls; and

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

We did not perform procedures to determine the operating effectiveness of controls for any period. Accordingly, we express no opinion on the operating effectiveness of any aspects of CHT's controls, individually or in the aggregate.

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

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

Suitability of controls

The suitability of the design of the 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 suitability of the design of the controls at individual subscriber and relying party locations.

Inherent limitations

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

Opinion

In our opinion, as of 22 February, 2019, CHT management's assertion, as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3.

This report does not include any representation as to the quality of CHT's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3, nor the suitability of any of CHT's services for any customer's intended purpose.

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

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

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

February 22, 2019

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 – HiPKI Root and Intermediate CAs within the Audit Report Scope

HiPKI Root CA - G1	**Root CA Certificate**	
	Subject	Issuer
	CN = HiPKI Root CA - G1 O = Chunghwa Telecom Co., Ltd. C = TW	CN = HiPKI Root CA - G1 O = Chunghwa Telecom Co., Ltd. C = TW
	Certificate related Information	Key Related Information
	Serial Number: 2d:dd:ac:ce:62:97:94:a1:43:e8:b0:cd:76:6a:5e:60 Signature Algorithm: sha256RSA Not Before: 2019-02-22 05:46:04 p.m. (UTC +8:00) Not After : 2037-12-31 11:59:59 p.m. (UTC +8:00) Thumbprint Algorithm: sha1 Thumbprint: 6a:92:e4:a8:ee:1b:ec:96:45:37:e3:29:57:49:cd:96:e3:e5:d2:60 Thumbprint Algorithm: sha256 Thumbprint: f0:15:ce:3c:c2:39:bf:ef:06:4b:e9:f1:d2:c4:17:e1:a0:26:4a:0a:94:be:1f:0c:8d:12:18:64:eb:69:49:cc	Subject Public Key: RSA(4096 bits) Subject Key Identifiers: f2:77:17:fa:5e:a8:fe:f6:3d:71:d5:68:ba:c9:46:0c:38:d8:af:b0
	Additional Information	Remark
	■ URL of HiPKI Repository for Certificate Policy and Certification Practice Statement Distribution: http://eca.hinet.net/repository-h	■ Self-signed by 1st Generation of HiPKI Root CA - G1.
HiPKI EV TLS CA - G1	**Intermediate CA Certificate**	
	Subject	Issuer
	CN = HiPKI EV TLS CA - G1 O = Chunghwa Telecom Co., Ltd. C = TW	CN = HiPKI Root CA - G1 O = Chunghwa Telecom Co., Ltd. C = TW
	Certificate related Information	Key Related Information

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

	Serial Number: 3c:43:cd:cd:dc:f2:3b:00:4f:0e:a0:73:fc:3e:a3:89 Signature Algorithm: sha256RSA Not Before: 2019-02-22 05:56:03 p.m. (UTC +8:00) Not After : 2037-12-31 11:59:59 p.m. (UTC +8:00) Thumbprint Algorithm: sha1 Thumbprint: 98:7e:11:0f:a2:3e:88:82:89:47:65:19:47:2f:40:2f:1e:42:28:37 Thumbprint Algorithm: sha256 Thumbprint: 2a:8e:6a:86:e7:4d:10:ed:b2:02:6c:81:69:3d:64:95:7a:0f:08:1c:16:31:91:2a:c9:5e:fd:fc:b5:62:56:57	Subject Public Key: RSA(4096 bits) Authority Key Identifiers: f2:77:17:fa:5e:a8:fe:f6:3d:71:d5:68:ba:c9:46:0c:38:d8:af:b0 Subject Key Identifiers: a9:0d:ea:63:ae:e3:8c:03:40:e7:ff:dc:33:28:e5:23:8e:cb:10:9b 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/HRCA_G1/CA.crl ■ Certificate Policy: [1]2.23.140.1.1 ■ URL of HiPKI Repository for Certificate Policy and Certification Practice Statement Distribution: http://eca.hinet.net/repository-h	■ CA certificate of 1st Generation of HiPKI EV TLS CA signed by HiPKI Root CA - G1.

中華電信

MANAGEMENT'S ASSERTION

Chunghwa Telecom (CHT) operates the Certification Authority (CA) services known as HiPKI Root CA - G1 and HiPKI EV TLS CA - G1 and provides extended validation SSL(EV SSL) CA services. CHT management has assessed its controls over its CA services. Based on that assessment, in providing its CA services at Taipei and Taichung, Taiwan, as of 22 February 2019 for its CAs as enumerated in Appendix A, CHT has:

- disclosed its SSL certificate lifecycle management business practices in its:
  - HiPKI EV TLS CA Certification Practice Statement Version 1.0;
  - HiPKI Root Certification Authority Certification Practice Statement Version 1.0; and
  - HiPKI Certificate Policy Version 1.0

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

- suitably designed, and placed into operation, controls to provide reasonable assurance that:
  - the integrity of keys and EV SSL certificates it manages is established and protected throughout their lifecycles; and
  - EV SSL subscriber information is properly authenticated (for the registration activities performed by CHT)

- suitably designed, and placed into operation, controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorized individuals;
  - the continuity of key and certificate management operations is maintained; and

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

- suitably designed, and placed into operation, controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3.

Signature: Chung, Ming

Title: Principal Engineer

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

<table>
<tr><td rowspan="5">HiPKI Root CA - G1</td><td colspan="2">Root CA Certificate</td></tr>
<tr><td>Subject</td><td>Issuer</td></tr>
<tr><td>CN = HiPKI Root CA - G1
O = Chunghwa Telecom Co., Ltd.
C = TW</td><td>CN = HiPKI Root CA - G1
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:
2d:dd:ac:ce:62:97:94:a1:43:e8:b0:cd:76:6a:5e:60
Signature Algorithm: sha256RSA
Not Before: 2019-02-22 05:46:04 p.m. (UTC +8:00)
Not After : 2037-12-31 11:59:59 p.m. (UTC +8:00)
Thumbprint Algorithm: sha1
Thumbprint:
6a:92:e4:a8:ee:1b:ec:96:45:37:e3:29:57:49:cd:96:e3:e5:d2:60
Thumbprint Algorithm: sha256
Thumbprint:
f0:15:ce:3c:c2:39:bf:ef:06:4b:e9:f1:d2:c4:17:e1:a0:26:4a:0a:94:be:1f:0c:8d:12:18:64:eb:69:49:cc</td><td>Subject Public Key: RSA(4096 bits)
Subject Key Identifiers:
f2:77:17:fa:5e:a8:fe:f6:3d:71:d5:68:ba:c9:46:0c:38:d8:af:b0</td></tr>
<tr><td>Additional Information
■ URL of HiPKI Repository for Certificate Policy and Certification Practice Statement Distribution: http://eca.hinet.net/repository-h</td><td>Remark
■ Self-signed by 1st Generation of HiPKI Root CA - G1.</td></tr>
<tr><td rowspan="4">HiPKI EV TLS CA - G1</td><td colspan="2">Intermediate CA Certificate</td></tr>
<tr><td>Subject</td><td>Issuer</td></tr>
<tr><td>CN = HiPKI EV TLS CA - G1
O = Chunghwa Telecom Co., Ltd.
C = TW</td><td>CN = HiPKI Root CA - G1
O = Chunghwa Telecom Co., Ltd.
C = TW</td></tr>
<tr><td>Certificate related Information</td><td>Key Related Information</td></tr>
</table>

	Serial Number: 3c:43:cd:cd:dc:f2:3b:00:4f:0e:a0:73:fc:3e:a3:89 Signature Algorithm: sha256RSA Not Before: 2019-02-22 05:56:03 p.m. (UTC +8:00) Not After : 2037-12-31 11:59:59 p.m. (UTC +8:00) Thumbprint Algorithm: sha1 Thumbprint: 98:7e:11:0f:a2:3e:88:82:89:47:65:19:47:2f:40:2f:1e:42:28:37 Thumbprint Algorithm: sha256 Thumbprint: 2a:8e:6a:86:e7:4d:10:ed:b2:02:6c:81:69:3d:64:95:7a:0f:08:1c:16:31:91:2a:c9:5e:fd:fc:b5:62:56:57	Subject Public Key: RSA(4096 bits) Authority Key Identifiers: f2:77:17:fa:5e:a8:fe:f6:3d:71:d5:68:ba:c9:46:0c:38:d8:af:b0 Subject Key Identifiers: a9:0d:ea:63:ae:e3:8c:03:40:e7:ff:dc:33:28:e5:23:8e:cb:10:9b 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/HRCA_G1/CA.crl ■ Certificate Policy: [1]2.23.140.1.1 ■ URL of HiPKI Repository for Certificate Policy and Certification Practice Statement Distribution: http://eca.hinet.net/repository-h	■ CA certificate of 1st Generation of HiPKI EV TLS CA signed by HiPKI Root CA - G1.