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):

Scope

We have been engaged, in a reasonable assurance engagement, to report on CHT management's assertion that in generating and protecting its HiPKI Root CA - G1 and HiPKI TLS CA - G1 on 22 February at Taipei, Taiwan, with the following identifying information:

CA Name	Subject Key Identifier	Certificate Serial Number
HiPKI Root CA - G1	f2:77:17:fa:5e:a8:fe:f6:3d:71:d5:68:ba:c9:46:0c:38:d8:af:b0	2d:dd:ac:ce:62:97:94:a1:43:e8:b0:cd:76:6a:5e:60
HiPKI EV TLS CA - G1	a9:0d:ea:63:ae:e3:8c:03:40:e7:ff:dc:33:28:e5:23:8e:cb:10:9b	3c:43:cd:cd:dc:f2:3b:00:4f:0e:a0:73:fc:3e:a3:89

CHT has:

- followed the CA key generation and protection requirements 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

- included appropriate, detailed procedures and controls in its HiPKI Root CA - G1 and HiPKI TLS CA - G1 Key Generation Script(s) approved on 18 February, 2019

- maintained effective controls to provide reasonable assurance that the HiPKI Root CA - G1 and HiPKI TLS CA - G1 were generated and protected in conformity with the procedures described in its CP/CPS and its Key Generation Script(s)

- performed, during the root key generation process, all procedures required by the Key Generation Script(s)

- generated the CA keys in a physically secured environment as described in its CP/CPS

- generated the CA keys using personnel in trusted roles under multiple person control and split knowledge

- generated the CA keys within cryptographic modules meeting the applicable technical and business requirements as disclosed in its CP/CPS

in accordance with CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.1.

Certification authority's responsibilities

CHT's management is responsible for its assertion, including the fairness of its presentation, and for generating and protecting its CA keys in accordance with CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.1.

Our independence and quality control

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* issued by the

International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

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

Auditor’s responsibilities

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

(1) obtaining an understanding of CHT’s documented plan of procedures to be performed for the generation of the certification authority key pairs for the HiPKI Root CA and HiPKI TLS CA; evaluating the suitability of the design of the controls; and

(2) reviewing the detailed Key Generation Script(s) for conformance with industry standard practices;

(3) testing and evaluating, during the key generation process, the effectiveness of controls over the integrity, confidentiality, and availability of all private keys, including back-up copies, and access

keys (including physical keys, tokens, and passwords), used in the establishment of the service;

(4) physical observation of all procedures performed during the key generation process to ensure that the procedures actually performed on 22 February 2019 were in accordance with the Key Generation Script(s) for the HiPKI Root CA and HiPKI TLS CA; and

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

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

Opinion

In our opinion, on 22 February 2019, CHT management's assertion, as referred to above, is fairly stated, in all material respects, in accordance with CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.1.

This report does not include any representation as to the quality of CHT's services beyond those covered by CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.1, nor the suitability of any of CHT's services for any customer's intended purpose.

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

February 22, 2019

DFK INTERNATIONAL

MANAGEMENT'S ASSERTION

Chunghwa Telecom (CHT) has deployed a public key infrastructure. As part of this deployment, it was necessary to create a hierarchy consistent of self-signed Root CAs and Intermediate CAs known as HiPKI Root CA - G1 and HiPKI EV TLS CA - G1. These CAs will serve as a Root CA and an Intermediate CA for client certificate services. In order to allow the CAs to be installed in a final production configuration, a Key Generation Ceremony was conducted, the purpose of which was to formally witness and document the creation of the CAs' private signing key. This helps assure the non-refutability of the integrity of the CHT HiPKI Root CA - G1 and HiPKI EV TLS CA - G1 key pairs, and in particular, the private signing keys.

CHT management has securely generated key pairs, each consisting of a public and private key, in support of its CA operations. The key pairs were generated in accordance with procedures described in CHT's Certificate Policy (CP) and Certification Practice Statement (CPS), and its Key Generation Script(s), which are in accordance with CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.1.

CHT management established and maintained effective controls over the generation of these keys. These controls were designed to provide reasonable assurance of adherence to the above-mentioned practices throughout the root key generation process.

CHT management is responsible for establishing and maintaining procedures over its CA key generations, and over the integrity and confidentiality of all private keys and access keys (including physical keys, tokens, and passwords) used in the establishment of the HiPKI Root CA - G1 and HiPKI EV TLS CA - G1, and for the CA environment controls relevant to the generation and protection of its CA keys.

CHT management has assessed the procedures and controls for the generation of the HiPKI Root CA - G1 and HiPKI EV TLS CA - G1 keys. Based on that assessment, in management’s opinion, in generation and protecting its CA keys for the HiPKI Root CA - G1 and HiPKI EV TLS CA - G1 on 22 February 2019 at Taipei, Taiwan, with the following identifying information:

CA Name	Subject Key Identifier	Certificate Serial Number
HiPKI Root CA - G1	f2:77:17:fa:5e:a8:fe:f6:3d:71:d5:68:ba:c9:46:0c:38:d8:af:b0	2d:dd:ac:ce:62:97:94:a1:43:e8:b0:cd:76:6a:5e:60
HiPKI EV TLS CA - G1	a9:0d:ea:63:ae:e3:8c:03:40:e7:ff:dc:33:28:e5:23:8e:cb:10:9b	3c:43:cd:cd:dc:f2:3b:00:4f:0e:a0:73:fc:3e:a3:89

CHT has:

- followed the CA key generation and protection requirements 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

- included appropriate, detailed procedures and controls in its HiPKI Root CA - G1 and HiPKI EV TLS CA - G1 Key Generation Script(s) approved on 18 February, 2019

- maintained effective controls to provide reasonable assurance that the HiPKI Root CA - G1 and HiPKI EV TLS CA - G1 were generated and protected in conformity with the procedures described in its CP/CPS and its Key Generation Script(s)

- performed, during the root key generation process, all procedures required by the Key Generation Script(s)

- generated the CA keys in a physically secured environment as described in its CP/CPS

- generated the CA keys using personnel in trusted roles under multiple person control and split knowledge

- generated the CA keys within cryptographic modules meeting the applicable technical and business requirements as disclosed in its CP/CPS

in accordance with CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.1.

Signature: Chung, Ming

Title: Principal Engineer.