Government TLS CA Management Assertion

July 17, 2019

The National Development Council（NDC）operates the Certification Authorities（CAs） services known as Government TLS Certification Authority（GTLSCA） and provides the following services:

- Subscriber registration
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation

The management of the NDC is responsible for establishing controls over its CA operations, including its CA business practices disclosure on GCA website [link], CA business practices management, CA environmental controls, CA key lifecycle management controls, subscriber key lifecycle management controls, and certificate lifecycle management 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, controls placed into operation can only provide reasonable assurance with respect to GTLSCA's Certification Authority operations.

NDC management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, , in GTLSCA management's opinion, in providing its CA services at at Taipei and Taichung, Taiwan as of July 10, 2019, for its CA：

CA Name	Key Hash
GTLSCA	D6EB2D9D61FE2BBB70882EB807B159B0F483226A

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
  - GTLSCA Certification Practice Statement V1.0; and
  - Chunghwa Telecom ecommerce Public Key Infrastructure (ePKI) Policy V1.7
- suitably designed, and placed into operation, controls to provide reasonable assurance that:
  - GTLSCA provides its services in accordance with GTLSCA's Certification Practice Statement

- suitably designed, and placed into operation, controls to provide reasonable assurance that: o the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
  - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles;
  - subscriber information is properly authenticated for the registration activities performed by GSSLCA; and
- suitably designed, and placed into operation, controls to provide reasonable assurance that: o logical and physical access to CA systems and data is restricted to authorised individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorised and performed to maintain CA systems integrity

in accordance with the WebTrust Principles and Criteria for Certification Authorities V2.1, including the following:

- CA Business Practices Disclosure
  - Certification Practice Statement (CPS)
- CA Business Practices Management
  - Certification Practice Statement Management
- CA Environmental Controls
  - Security Management

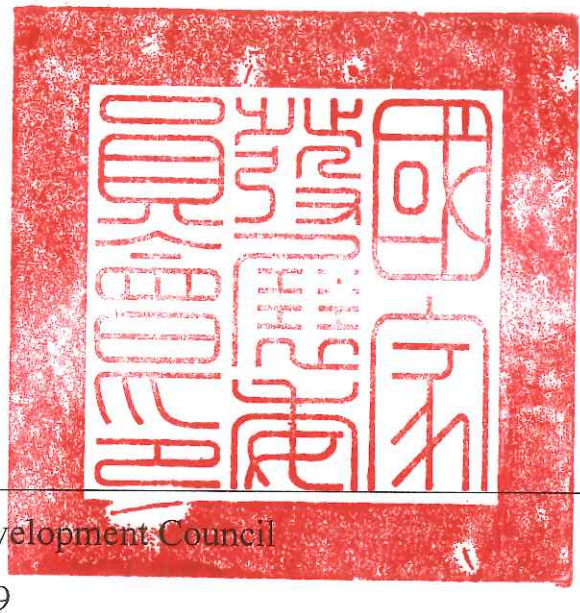
- Asset Classification and Management
- Personnel Security
- Physical & Environmental Security
- Operations Management
- System Access Management
- System Development and Maintenance
- Business Continuity Management
- Monitoring and Compliance
- Audit Logging

■ CA Key Lifecycle 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 Lifecycle Management

■ Certificate Lifecycle Management Controls

- Subscriber Registration
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Validation



National Development Council

July 17, 2019

Independent Assurance Report

To the management of the National Development Council：

Scope

We have been engaged, in a reasonable assurance engagement, to report on National Development Council (NDC) management's assertion that for its Certification Authority (CA) operations at Taipei and Taichung, Taiwan, for its CA:

CA Name	Key Hash
GTLSCA	D6EB2D9D61FE2BBB70882EB807B159B0F483226A

The NDC has：

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
  - Government TLS Certification Authority Certification (GTLSCA) Practice Statement V1.0; and
- suitably designed, and placed into operation, controls to provide reasonable assurance that:
  - the integrity of keys it manages is established and protected throughout their lifecycles;
- 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

in accordance with the WebTrust Principles and Criteria for Certification Authorities V2.1.

GTLSCA do not escrow its CA keys, and does not provide subscriber key generation services. Accordingly, our procedures did not extend to controls that would address those criteria.

Due to the GTLSCA has not sign any formal certificates, the integrity of subscriber keys and subscriber authentication information are not covered in this audit.

Certification authority's responsibilities

NDC's management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with 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 behavior.

The firm applies International Standard on Quality Control, 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 attestation standards established by the American Institute of Certified Public Accountants/CPA Canada. 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 GTLSCA's key[1] life cycle management business and its controls over key integrity, over the authenticity and confidentiality of subscriber and relying party information, over the continuity of key 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.

[1] GTLSCA's certificate has not signed by CHT's Root CA & not covered in this audit.

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 GTLSCA's controls, individually or in the aggregate.

Suitability of controls

The suitability of the design of the controls at GTLSCA 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, GTLSCA'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 July 17, 2019, GTLSCA management's assertion, as referred to above except that is not covered in audit scope, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities V2.1.

This report does not include any representation as to the quality of GTLSCA's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities V2.1, nor the suitability of any of GTLSCA's services for any customer's intended purpose.

KPMG

KPMG
Certified Public Accountants
Taipei, Taiwan, ROC
July 17, 2019