



## Government TLS CA Management Assertion

**July 17, 2019**

The National Development Council (NDC) operates the Certification Authority (CA) services known as Government TLS Certification Authority (GTLSCA) in scope for SSL Baseline Requirements and Network Security Requirements and provides SSL CA services. NDC management has assessed its disclosures of its certificate practices and controls over its SSL CA services. Based on that assessment, in providing its SSL Certification Authority (CA) services at Taipei and Taichung, Taiwan as of July 10, 2019, for its CA :

CA Name	Key Hash
GTLSCA	D6EB2D9D61FE2BBB70882EB807B159B0F483226A

NDC has:

- disclosed its SSL certificate lifecycle management business practices in its:
  - GTLSCA Certification Practice Statement V1.0; and
  - Chunghwa Telecom ecommerce Public Key Infrastructure (ePKI) Policy V1.7

including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirement on the GTLSCA/GCA 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<sup>1</sup> 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<sup>2</sup> 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.

---

<sup>1</sup> GTLSCA has not issued any SSL certificates, SSL certificates and subscriber register information authentication are not included in this audit.

<sup>2</sup> Same as 1



---

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 as 10 July 2019, for its CA in scope for SSL Baseline Requirements and Network Security Requirements.

CA Name	Key Hash
GTLSCA	D6EB2D9D61FE2BBB70882EB807B159B0F483226A

The NDC has :

- disclosed its SSL certificate lifecycle management business practices in its:
  - Government TLS Certification Authority Certification (GTLSCA) Practice Statement V1.0including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirement on the GTLSCA/GCA 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<sup>1</sup> 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<sup>2</sup> 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.

---

<sup>1</sup> GTLSCA has not issued any SSL certificates, SSL certificates and subscriber register information authentication are not included in this audit.

<sup>2</sup> Same as 1



### **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 – 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.

### **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 GTLSCA's SSL certificate<sup>3</sup> lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of SSL certificates, and obtaining an understanding of GTLSCA's

---

<sup>3</sup> GTLSCA's certificate has not signed by CHT's Root CA & not covered in this audit.



network and certificate system security to meet the requirements set forth by the CA/Browser Forum;

- (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 GTLSCA'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.

### **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 – SSL Baseline with Network Security V2.3.

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 – SSL Baseline with Network Security V2.3, nor the suitability of any of GTLSCA's services for any customer's intended purpose.

A handwritten signature of the KPMG firm, written in a cursive, stylized font.

KPMG

Certified Public Accountants

Taipei, Taiwan, ROC

July 17, 2019