Independent assurance Report

To the management of the TAIWAN-CA INC.：

Scope

We have been engaged, in a reasonable assurance engagement, to report on TWCA management's assertion that for its Certification Authority (CA) operations at Taipei and Taichung, Taiwan, throughout the period January 1, 2019 to December 31, 2019 for its CAs as enumerated in Appendix, TWCA has:

- Disclosed its extended validation SSL certificate lifecycle management business practices in its:
  - TWCA Root Certification Authority Certification Practice Statement V1.3 drafted, effective from 15 May 2019; and
  - TWCA EV SSL Certification Authority Certification Practice Statement V1.4.1 drafted, effective from 20 June 2019; and
  - TWCA Public Key Infrastructure Policy V2.0

  including its commitment to provide EV SSL certificates in conformity with the CA/Browser Forum Guidelines on the TWCA website, and provided such services in accordance with its disclosed practices.
- Maintained effective 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 TWCA

- Maintained effective controls to provide reasonable assurance that:
  - requests for EV SSL certificates are properly authenticated; and
  - certificates issued to EV SSL Authorities are not valid for a period longer than specified by the CA/Browser Forum
  - maintained effective controls to provide reasonable assurance that its EV SSL Authority is operated in conformity with CA/Browser Forum Guidelines

in accordance with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL Version 1.6.8.

Certification authority's responsibilities

TWCA'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 - Extended Validation SSL Version 1.6.8.

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 assertion based on our examination. Our examination was conducted 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 TWCA's EV SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of EV SSL certificates;

(2) selectively testing transactions executed in accordance with disclosed EV SSL certificate lifecycle management 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 the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Relative effectiveness of controls

The relative effectiveness and significance of specific controls at TWCA 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.

Inherent limitations

Because of the nature and inherent limitations of controls, TWCA'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, throughout the period January 1, 2019 to December 31, 2019, TWCA management's assertion, as referred to above, is fairly stated, in all material respects, in accordance with WebTrust Principles

and Criteria for Certification Authorities - Extended Validation SSL Version 1.6.8.

This report does not include any representation as to the quality of TWCA's services beyond those covered by WebTrust Principles and Criteria for Certification Authorities - Extended Validation SSL Version 1.6.8, nor the suitability of any of TWCA's services for any customer's intended purpose.

Use of the WebTrust seal

TWCA's use of the WebTrust for Certification Authorities – Extended Validation SSL 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.

KPMG

Certified Public Accountants

Taipei, Taiwan, ROC

February 24, 2020

Appendix A – List of Root and Subordinate CAs in Scope

TWCA Global Root CA	TWCA Global Root CA
	Subject
	CN = TWCA Global Root CA OU = Root CA O = TAIWAN-CA C = TW
	Certificate Related Information
	Serial Number 0cbe Signature Algorithm: sha256RSA Not Before: 2012-Jun-27 14:28:33 Not After: 2030-Dec-31 23:59:59 Thumbprint Algorithm: sha1 Thumbprint 9cbb4853f6a4f6d352a4e83252556013f5adaf65
	Issuer
	CN = TWCA Global Root CA OU = Root CA O = TAIWAN-CA C = TW
	Key Related Information
	Subject Public Key: RSA(4096 bits) Subject Key Identifiers:

TWCA Root Certification Authority	TWCA Root Certification Authority
	Subject
	CN = TWCA Root Certification Authority OU = Root CA O = TAIWAN-CA C = TW
	Certificate Related Information
	Serial Number 01 Signature Algorithm: sha256RSA Not Before: 2008-Aug-28 03:47:13 Not After: 2030-Dec-31 23:59:59 Thumbprint Algorithm: sha1 Thumbprint df646dcb7b0fd3a96aee88c64e2d676711ff9d5f
	Issuer
	CN = TWCA Root Certification Authority OU = Root CA O = TAIWAN-CA C = TW
	Key Related Information
	Subject Public Key: RSA(4096 bits) Subject Key Identifiers: c8 44 5a fe 7f fd a9 9b 86 35 be e2 a5 f6 19 fb 5e bf 6f 59 Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)

TWCA Root Certification Authority	TWCA Root Certification Authority(2048)
	Subject
	CN = TWCA Root Certification Authority OU = Root CA O = TAIWAN-CA C = TW
	Certificate Related Information
	Serial Number 01 Signature Algorithm: sha1RSA Not Before: 2008-Aug-28 15:24:33 Not After: 2030-Dec-31 23:59:59 Thumbprint Algorithm: sha1 Thumbprint cf9e876dd3ebfc422697a3b5a37aa076a9062348
	Issuer
	CN = TWCA Root Certification Authority OU = Root CA O = TAIWAN-CA C = TW
	Key Related Information
	Subject Public Key: RSA(2048 bits) Subject Key Identifiers: 6a 38 5b 26 8d de 8b 5a f2 4f 7a 54 83 19 18 e3 08 35 a6 ba Basic Constraint: Subject Type=CA Path Length Constraint=None Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)

TWCA Global Root CA	TWCA Global Root CA(4096)
	Subject
	CN = TWCA Global Root CA OU = Root CA O = TAIWAN-CA C = TW
	Certificate Related Information
	Serial Number 40013353e40000000000000cca5d1b69 Signature Algorithm: sha256RSA Not Before: 2014-Oct-28 15:38:31 Not After: 2030-Dec-31 23:59:59 Thumbprint Algorithm: sha1 Thumbprint fd54e4643b49705a2aaae50653c4f56c2df8083d
	Issuer
	CN = TWCA Root Certification Authority OU = Root CA O = TAIWAN-CA C = TW
	Key Related Information
	Subject Public Key: RSA(2048 bits) Subject Key Identifiers: 6a 38 5b 26 8d de 8b 5a f2 4f 7a 54 83 19 18 e3 08 35 a6 ba Basic Constraint: Subject Type=CA Path Length Constraint=None Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)

TWCA Global EVSSL Certification Authority	TWCA Global EVSSL Certification Authority
	Subject
	CN = TWCA Global EVSSL Certification Authority OU = Global EVSSL Sub-CA O = TAIWAN-CA C = TW
	Certificate Related Information
	Serial Number 40013304f70000000000000cc042cd6d Signature Algorithm: sha256RSA Not Before: 2012-Aug-23 17:53:30 Not After: 2030-Aug-23 23:59:59 Thumbprint Algorithm: sha1 Thumbprint 071a25fa76a200da3c53f1ee791e7b627d32c349
	Issuer
	CN = TWCA Global Root CA OU = Root CA O = TAIWAN-CA C = TW
	Key Related Information
	Subject Public Key:RSA(2048 bits) Authority Key Identifiers: 48 db cd de 8e e9 49 72 5a 88 e8 b1 d8 3d 07 b3 b9 6b 66 50 Subject Key Identifiers: e4 6e bd a1 2b ce e4 c2 d5 28 74 5c bd d9 8c 6f 04 72 2a 06 de Basic Constraint: Subject Type=CA Path Length Constraint=0 Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)

TWCA EVSSL Certification Authority	TWCA EVSSL Certification Authority
	Subject
	CN = TWCA EVSSL Certification Authority OU = EVSSL Sub-CA O = TAIWAN-CA C = TW
	Certificate Related Information
	Serial Number 400132dd120000000000000cc1e1f977 Signature Algorithm: sha1RSA Not Before: 2011-Jun-10 10:49:38 Not After: 2021-Jun-10 23:59:59 Thumbprint Algorithm: sha1 Thumbprint 29429d028287a76c6c236e195e237e2407cd291d
	Issuer
	CN = TWCA Root Certification Authority OU = Root CA O = TAIWAN-CA C = TW
	Key Related Information
	Subject Public Key: RSA(2048 bits) Authority Key Identifiers: 6a 38 5b 26 8d de 8b 5a f2 4f 7a 54 83 19 18 e3 08 35 a6 ba Subject Key Identifiers: b9 2c 09 b5 34 2a f9 fe 5c 0d fd 6f 76 8b d5 92 1a e4 61 56 Basic Constraint: Subject Type=CA Path Length Constraint=0 Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)