KPMG

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, 2018 to December 31, 2018 for its CAs as enumerated in Appendix for SSL Baseline Requirements and Network Security Requirements, TWCA has:

- Disclosed its SSL certificate lifecycle management business practices in its:
  - TWCA Root Certification Authority Certification Practice Statement V1.2; and
  - TWCA Global Certification Authority Certification Practice Statement V1.4(draft, Effective from March 1, 2018); and
  - TWCA Public Key Infrastructure Policy V2.0

  including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements 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 SSL certificates it manages is established and protected throughout their lifecycles; and
- SSL subscriber information is properly authenticated for the registration activities performed by TWCA.

- Maintained effective 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
- maintained effective 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 V2.2.

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 for Certification Authorities – SSL Baseline with Network Security Version V2.2.

KPMG

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.

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 TWCA's SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of SSL certificates, and obtaining an understanding of TWCA's network and certificate system security to meet the requirements set forth by the CA/Browser Forum;

(2) selectively testing transactions executed in accordance with

disclosed 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, 2018 to December 31, 2018, TWCA 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 V2.2.

This report does not include any representation as to the quality of TWCA's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security V2.2, 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 – SSL Baseline with Network Security 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

KPMG
Certified Public Accountants
Taipei, Taiwan, ROC
February 27, 2019

Appendix A – List of Root and Subordinate CAs in Scope

	TWCA Global Root CA	
TWCA Global Root CA	Subject	Issuer
	CN = TWCA Global Root CA OU = Root CA O = TAIWAN-CA C = TW	CN = TWCA Global Root CA OU = Root CA O = TAIWAN-CA C = TW
	Certificate Related Information	Key Related Information
	Serial Number: 0c be Signature Algorithm: sha256RSA Not Before: 2012-Jun-27 14:28:33 Not After: 2030-Dec-31 23:59:59 Thumbprint Algorithm: sha1 Thumbprint: 9c bb 48 53 f6 a4 f6 d3 52 a4 e8 32 52 55 60 13 f5 ad af 65	Subject Public Key: RSA(4096 bits) Subject Key Identifiers:

	TWCA Root Certification Authority	
TWCA Root Certification Authority	Subject	Issuer
	CN = TWCA Root Certification Authority OU = Root CA O = TAIWAN-CA C = TW	CN = TWCA Root Certification Authority OU = Root CA O = TAIWAN-CA C = TW
	Certificate Related Information	Key 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: df 64 6d cb 7b 0f d3 a9 6a ee 88 c6 4e 2d 67 67 11 ff 9d 5f	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	Issuer
	CN = TWCA Root Certification Authority OU = Root CA O = TAIWAN-CA C = TW	CN = TWCA Root Certification Authority OU = Root CA O = TAIWAN-CA C = TW
	Certificate Related Information	Key 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: cf 9e 87 6d d3 eb fc 42 26 97 a3 b5 a3 7a a0 76 a9 06 23 48	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	Issuer
	CN = TWCA Global Root CA OU = Root CA O = TAIWAN-CA C = TW	CN = TWCA Root Certification Authority OU = Root CA O = TAIWAN-CA C = TW
	Certificate Related Information	Key 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: fd 54 e4 64 3b 49 70 5a 2a aa e5 06 53 c4 f5 6c 2d f8 08 3d	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 Secure SSL Certification Authority	
	Subject	Issuer
	CN = TWCA Secure SSL Certification Authority OU = Secure SSL Sub-CA O = TAIWAN-CA C = TW	CN = TWCA Global Root CA OU = Root CA O = TAIWAN-CA C = TW
	Certificate Related Information	Key Related Information
TWCA Secure SSL Certification Authority	Serial Number: 40 01 33 53 e4 00 00 00 00 00 0c c3 6e 88 8d Signature Algorithm: sha256RSA Not Before: 2014-Oct-28 15:27:56 Not After: 2024-Oct-28 23:59:59 Thumbprint Algorithm: sha1 Thumbprint: 0a 72 ef d6 60 fd 34 f2 54 e6 6a 85 95 ba 81 e6 0a 75 4e 68	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: f8 07 c2 68 24 ff 85 95 cb db 1e e3 33 9c 2a 4f 97 20 56 7b Basic Constraint: Subject Type=CA Path Length Constraint=0 Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)

	TWCA Global EVSSL Certification Authority	
	Subject	Issuer
	CN = TWCA Global EVSSL Certification Authority OU = Global EVSSL Sub-CA O = TAIWAN-CA C = TW	CN = TWCA Global Root CA OU = Root CA O = TAIWAN-CA C = TW
	Certificate Related Information	Key Related Information
TWCA Global EVSSL Certification Authority	Serial Number: 40 01 33 04 f7 00 00 00 00 00 0c c0 42 cd 6d Signature Algorithm: sha256RSA Not Before: 2012-Aug-23 17:53:30 Not After: 2030-Aug-23 23:59:59 Thumbprint Algorithm: sha1 Thumbprint: 07 1a 25 fa 76 a2 00 da 3c 53 f1 ee 79 1e 7b 62 7d 32 c3 49	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	
	Subject	Issuer
	CN = TWCA EVSSL Certification Authority OU = EVSSL Sub-CA O = TAIWAN-CA C = TW	CN = TWCA Root Certification Authority OU = Root CA O = TAIWAN-CA C = TW
	Certificate Related Information	Key Related Information
TWCA EVSSL Certification Authority	Serial Number: 40 01 32 dd 12 00 00 00 00 00 0c c1 e1 f9 77 Signature Algorithm: sha1RSA Not Before: 2011-Jun-10 10:49:38 Not After: 2021-Jun-10 23:59:59 Thumbprint Algorithm: sha1 Thumbprint: 29 42 9d 02 82 87 a7 6c 6c 23 6e 19 5e 23 7e 24 07 cd 29 1d	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)

	TWCA InfoSec User CA	
	Subject	Issuer
	CN = TWCA InfoSec User CA OU = User CA O = TAIWAN-CA Inc. C = TW	CN = TWCA Root Certification Authority OU = Root CA O = TAIWAN-CA C = TW
	Certificate Related Information	Key Related Information
TWCA InfoSec User CA	Serial Number: 40 01 33 04 20 00 00 00 00 00 0c c2 90 1d 53 Signature Algorithm: sha1RSA Not Before: 2012-Jun-8 09:51:19 Not After: 2022-Jun-8 23:59:59 Thumbprint Algorithm: sha1 Thumbprint: a2 5d 97 6f 92 d8 9c 9c dd 6f 57 b1 b8 0b 51 f5 6e 00 42 f9	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: 21 20 6a 92 e9 69 5b ac c8 63 eb 64 ce 82 c1 51 66 2a 87 e2 Basic Constraint: Subject Type=CA Path Length Constraint=0 Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)

	Subordinate CA Certificate	
	Subject	Issuer
	CN = TWCA InfoSec User CA OU = User CA O = TAIWAN-CA Inc. C = TW	CN = TWCA Root Certification Authority OU = Root CA O = TAIWAN-CA C = TW
	Certificate Related Information	Key Related Information
TWCA InfoSec User CA	Serial Number: 40 01 33 53 e4 00 00 00 00 00 0c c9 71 38 a0 Signature Algorithm: sha256RSA Not Before: 2014-Oct-28 02:48:11 Not After: 2024-Oct-28 23:59:59 Thumbprint Algorithm: sha1 Thumbprint: 58 e9 11 0c d6 60 36 33 7f 7e 0d 46 cb be 94 58 7f ae 0e 19	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: d9 10 f0 de c2 a1 99 f5 7e 4b 93 a2 13 c6 d6 46 73 c2 49 de Basic Constraint: Subject Type=CA Path Length Constraint=0 Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)

	TWCA InfoSec User CA	
	Subject	Issuer
	CN = TWCA InfoSec User CA OU = User CA O = TAIWAN-CA Inc. C = TW	CN = TWCA Root Certification Authority OU = Root CA O = TAIWAN-CA C = TW
	Certificate Related Information	Key Related Information
TWCA InfoSec User CA	Serial Number: 40 01 33 f0 14 00 00 00 00 00 0c cf ae 3c d7 Signature Algorithm: sha1RSA Not Before: 2018-Oct-12 11:03:57 Not After: 2028-Oct-12 23:59:59 Thumbprint Algorithm: sha1 Thumbprint: 91 0a 43 af dd 86 27 1f 30 dd 93 7e e6 ad 92 b1 32 44 34 d2	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: 46 6f 16 86 f4 a0 5b 11 41 be 93 6a ec 06 50 ce 8a 55 46 59 Basic Constraint: Subject Type=CA Path Length Constraint=0 Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)

	TWCA InfoSec User CA	
	Subject	Issuer
	CN = TWCA InfoSec User CA OU = User CA O = TAIWAN-CA Inc. C = TW	CN = TWCA Global Root CA OU = Root CA O = TAIWAN-CA C = TW
	Certificate Related Information	Key Related Information
TWCA InfoSec User CA	Serial Number: 40 01 33 f0 14 00 00 00 00 00 00 0c c7 02 41 af Signature Algorithm: sha256RSA Not Before: 2018-Oct-12 04:45:27 Not After: 2028- Oct-12 23:59:59 Thumbprint Algorithm: sha256 Thumbprint: 5b be 8e 29 0d ab 5c 98 4c 15 45 00 dd 16 37 9c b2 70 4d 20	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: 1a 7c e5 e7 6a 1f 61 8e 4b aa b6 fc fb f6 90 85 ee 84 09 fe Basic Constraint: Subject Type=CA Path Length Constraint=0 Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)