



Independent Assurance Report

To the management of the TAIWAN-CA INC. :

Scope

We have been engaged, in a reasonable assurance engagement, to report on TAIWAN-CA INC. (TWCA) management's assertion that for its Certification Authority (CA) operations at Taipei and Taichung, Taiwan throughout the period January 1, 2017 to December 31, 2017 for its CAs as enumerated in Appendix, the TWCA has :

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
 - TWCA Root Certification Authority Certification Practice Statement V1.2; and
 - TWCA Global Certification Authority Certification Practice Statement V1.3; and
 - TWCA EV SSL Certification Authority Certification Practice Statement V1.3; and
 - TWCA Public Key Infrastructure Policy V2.0
- Maintained effective controls to provide reasonable assurance that :
 - TWCA Certification Practice Statements are consistent with its Certificate Policy
 - TWCA provides its services in accordance with its



Certificate Policy and Certification Practice Statements

- Maintained effective controls to provide reasonable assurance that :
 - 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 TWCA; and
 - subordinate CA certificate requests are accurate, authenticated, and approved
- 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

in accordance with the WebTrust Principles and Criteria for Certification Authorities V2.0.

TWCA makes use of external registration authorities for specific subscriber registration activities as disclosed in TWCA's business practices. Our procedures did not extend to the controls exercised by these external registration authorities.



TWCA does 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.

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 WebTrust Principles and Criteria for Certification Authorities V2.0.

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 key and certificate life cycle management business and its controls over key and certificate integrity, over the authenticity and confidentiality of subscriber and relying party information, over the continuity of key and certificate lifecycle management operations and over development, maintenance and operation of systems integrity;
- (2) selectively testing transactions executed in accordance with disclosed key and certificate life cycle management business 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.

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, 2017 to December 31, 2017, the TWCA management assertion, as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities V2.0.

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 V2.0, 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 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.

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

KPMG

Certified Public Accountants

Taipei, Taiwan, ROC

March 9, 2018



TAIWAN-CA INC. Management's Assertion

The TAIWAN-CA INC. (TWCA) operates the Certification Authority (CA) services known as TWCA Root Certification Authority and TWCA Global Root Certification Authority, TWCA, Secure SSL Certification Authority, InfoSec Certification Authority and TWCA EVSSL Certification Authority. A full listing of the Root CAs and Subordinate CAs and their respective functions is in appendix to this assertion letter. TWCA provides the following CA services :

- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation
- Subordinate CA certification

The management of the TWCA is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure on its [website](#), CA business

practices management, CA environmental controls, CA key lifecycle management controls, subscriber key lifecycle management controls, certificate lifecycle management controls, and subordinate CA 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, even effective controls can only provide reasonable assurance with respect to TWCA's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

TWCA management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in TWCA management's opinion, in providing its Certification Authority (CA) services at in Taipei and Taichung, Taiwan, throughout the period January 1, 2017 to December 31, 2017, TWCA has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
 - TWCA Root Certification Authority Certification Practice Statement V1.2; and

- TWCA Global Certification Authority Certification Practice Statement V1.3; and
- TWCA EV SSL Certification Authority Certification Practice Statement V1.3; and
- TWCA Public Key Infrastructure Policy V2.0

■ maintained effective controls to provide reasonable assurance that:

- TWCA's Certification Practice Statements are consistent with its Certificate Policy
- TWCA provides its services in accordance with its Certificate Policy and Certification Practice Statements

■ Maintained effective controls to provide reasonable assurance that :

- 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 TWCA); and
- subordinate CA certificate requests are accurate, authenticated, and approved

■ Maintained effective controls to provide reasonable assurance that :

- 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 V2.0, including the following:

CA Business Practices Disclosure

- Certification Practice Statement (CPS)
- Certificate Policy (CP)

CA Business Practices Management

- Certificate Policy Management
- Certification Practice Statement Management
- CP and CPS Consistency

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

Subscriber Key Lifecycle Management Controls

- Integrated Circuit Card (ICC) Lifecycle Management

Certificate Lifecycle Management Controls

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

Subordinate CA Certificate Lifecycle Management Controls

- Subordinate CA Certificate Lifecycle Management

TWCA does not provide subscriber key generation services, and does not provide certificate suspension services. Accordingly, our assertion does not extend to controls that would address those criteria

Title: President

Signature *Lee Jang-Lin*

Date March 9, 2018

TAIWAN-CA INC. (TWCA)

10th Floor, 85 Yenping South Road, Taipei, Taiwan, R.O.C. 10043

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: 40013353e4000000000000cca5d1b69 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	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
	Serial Number: 40 01 33 53 e4 00 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	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
	Serial Number: 40 01 33 04 f7 00 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	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
	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	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
	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)

TWCA InfoSec User CA	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
	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)