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 its locations as detailed in Appendix A, throughout the period January 1, 2021 to December 31, 2021 for its CAs as enumerated in Appendix B, 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 V1.3, effective from 30 January 2020; and
  - TWCA Global Certification Authority Certification Practice Statement V1.6, effective from 21 December 2021; and
  - TWCA EV SSL Certification Authority Certification Practice Statement V1.6, effective from 21 December 2021; and
  - TWCA Public Key Infrastructure Certificate Policy V2.3
- 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 V2.2.1.

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 V2.2.1.

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.

KPMG Audit Team qualifications are listed in Appendix C.

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.

TWCA's management has disclosed to KPMG the incidents as detailed in Appendix D that have been posted in Bugzilla website that can be accessed publicly.

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, 2021 to December 31, 2021, 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 V2.2.1.

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 V2.2.1, 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 Principles and Criteria 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.

Chen, Pei Chi

KPMG

KPMG

Certified Public Accountants

Taipei, Taiwan, ROC

February 23, 2022

Appendix A – Locations

Country	City	Data Center Type
Taiwan	Taipei	Owned by TWCA
Taiwan	New Taipei	Outsourcing Data Center
Taiwan	Taichung	Outsourcing Data Center

Appendix B – 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 Thumbprint Algorithm:sha2 Thumbprint 59769007F7685D0FCD50872F9F95D5755A5B2B457D81F3692B610A98672F0E1B
	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(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 Thumb print Algorithm: sha2 Thumbprint BFD88FE1101C41AE3E801BF8BE56350EE9BAD1A6B9BD515EDC5C6D5B8711AC44
	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 Thumbprint Algorithm: sha2 Thumbprint 8AD47F6D70A44FA80AF0F931125FFE3A76876FFAD219A4D40A13C038DC85E69E
	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: 48 db cd de 8e e9 49 72 5a 88 e8 b1 d8 3d 07 b3 b9 6b 66 50 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
	CN = TWCA Secure SSL Certification Authority OU = Secure SSL Sub-CA O = TAIWAN-CA C = TW
	Certificate Related Information
	Serial Number 40013353e40000000000000cc36e888d Signature Algorithm: sha256RSA Not Before: 2014-Oct-28 15:27:56 Not After: 2024-Oct-28 23:59:59 Thumbprint Algorithm: sha1 Thumbprint 0a72efd660fd34f254e66a8595ba81e60a754e68 Thumbprint Algorithm: sha2 Thumbprint 9B16F2F680D7C4BD6A67F609340DA6416ABF9E43F1326B01B988192271D0B5F2
	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: 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
	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 Thumbprint Algorithm: sha2 Thumbprint 49695A5F0F7EF6EDF698193D99ED48BAADE20EA457403C11CEAD492C458665DA
	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 Thumbprint Algorithm: sha2 Thumbprint 7F1229B48517F2A66BAE4E2E342500F33B273A5CFCB625481C3783CA1F5366BC
	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)

TWCA InfoSec User CA	TWCA InfoSec User CA
	Subject
	CN = TWCA InfoSec User CA OU = User CA O = TAIWAN-CA Inc. C = TW
	Certificate Related Information
	Serial Number 400133042000000000000cc2901d53 Signature Algorithm: sha1RSA Not Before: 2012-Jun-8 09:51:19 Not After: 2022-Jun-8 23:59:59 Thumbprint Algorithm: sha1 Thumbprint a25d976f92d89c9cdd6f57b1b80b51f56e0042f9 Thumbprint Algorithm: sha2 Thumbprint A97CA1375B91953E536A55476B0AC444C7086A951E490A3A3D13630A19F40CD4
	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: 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	TWCA InfoSec User CA
	Subject
	CN = TWCA InfoSec User CA OU = User CA O = TAIWAN-CA Inc. C = TW
	Certificate Related Information
	Serial Number 40013353e40000000000000cc97138a0 Signature Algorithm: sha256RSA Not Before: 2014-Oct-28 02:48:11 Not After: 2024-Oct-28 23:59:59 Thumbprint Algorithm: sha1 Thumbprint 58e9110cd66036337f7e0d46cbbe94587fae0e19 Thumbprint Algorithm: sha2 Thumbprint 074840E3A67DCD2600B6B004E1187AC80BDFE896CAF493DF94CC3D9A3CA68814
	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: 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	TWCA InfoSec User CA
	Subject
	CN = TWCA InfoSec User CA OU = User CA O = TAIWAN-CA Inc. C = TW
	Certificate Related Information
	Serial Number 400133f0140000000000000ccfae3cd7 Signature Algorithm: sha1RSA Not Before: 2018-Oct-12 11:03:57 Not After: 2028-Oct-12 23:59:59 Thumbprint Algorithm: sha1 Thumbprint 910a43afdd86271f30dd937ee6ad92b1324434d2 Thumbprint Algorithm: sha2 Thumbprint C00A8183C9865A0847C01158F785A5F35DCB8B596C7BF46FD6497F72F02E5E32
	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: 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	TWCA InfoSec User CA
	Subject
	CN = TWCA InfoSec User CA OU = User CA O = TAIWAN-CA Inc. C = TW
	Certificate Related Information
	Serial Number 400133f0140000000000000cc70241af Signature Algorithm: sha256RSA Not Before: 2018-Oct-12 04:45:27 Not After: 2028- Oct-12 23:59:59 Thumbprint Algorithm: sha256 Thumbprint 5bbe8e290dab5c984c154500dd16379cb2704d20 Thumbprint Algorithm: sha2 Thumbprint BFAAF990B98D9168466A9F0757DC2F1614B9F938B3A74511B994A2B858E1490E
	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: 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)

Appendix C – Auditor Qualifications

KPMG provides assurance and attest reports as part of the Firm's regular business activities and the standards set out in the WebTrust Agreement ,and all practitioners/staff are experienced and well-skilled to conduct WebTrust for Certification Authorities audit.

Team Member	Title	Certifications	Years of Experience	Years of Experience with PKI
Team Leader	Partner	CISA,IRCA Registered ISO 27001 LA	More than 20 years	More than 10 years
Member A	Manager	CISA, ISO 27001 LA	More then 15 years	More then 11 years
Member B	Assistant Manager	CAMS, ISO 27001 LA	More then 6 years	More then 5 years
Member C	Senior Consultant	ISO 27001 LA	More then 6 years	More then 5 years
Member D	Senior Consultant	ISO 27001 LA	More then 5 years	More then 5 years

Appendix D – Publicly disclosed incidents

NO	Subject	Publicly Link
1	Taiwan-CA: Invalid stateOrProvinceName	Bugzilla Ticket Link
2	TWCA: CA Certificate Missing from Audit Reports	Bugzilla Ticket Link
3	TWCA: Policy OID not set to indicate the assurance level to the issued certs	Bugzilla Ticket Link