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 its locations as detailed in Appendix A, throughout the period January 1, 2024 to December 31, 2024 for its CAs as enumerated in Appendix B for SSL Baseline Requirements, TWCA has:

- disclosed its SSL certificate lifecycle management business practices in its:
  - TWCA Cyber Certification Authority Certification Practice Statement V1.1, effective from 29 February 2024; and
  - TWCA Public Key Infrastructure Certificate Policy V2.6.1, effective from 1 July 2024;

  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

in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline V2.8.

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 – SSL Baseline Version V2.8.

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 behaviour.

The firm applies International Standard on Quality Control 1, *Quality Control for Firms that Perform Audits and Reviews of Historical Financial Information, and Other Assurance and Related Services*, 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.

Practitioner'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 TWCA's SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of SSL certificates;
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.

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.

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

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. For example, because of their nature, controls may not prevent, or detect unauthorised access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection to the future of any conclusions based on our findings is subject to the risk that controls may become ineffective.

Opinion

In our opinion, throughout the period January 1, 2024 to December 31, 2024, 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 V2.8.

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 V2.8, 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 – SSL Baseline 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 26, 2025

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

1

TWCA CYBER Root CA	TWCA CYBER Root CA
	Subject
	CN = TWCA CYBER Root CA OU = Root CA O =TAIWAN-CA C = TW
	Certificate Related Information
	Serial Number 4001348cc200000000000000013cf2c6 Signature Algorithm: sha384RSA Not Before: 2022-Nov-22 14:54:29 Not After: 2047- Nov-22 23:59:59 Thumbprint Algorithm: sha1 Thumbprint f6b11c1a8338e97bdbb3a8c83324e02d9c7f2666 Thumbprint Algorithm: sha2 Thumbprint 3F63BB2814BE174EC8B6439CF08D6D56F0B7C405883A5648A334424D6B3EC558
	Issuer
	CN = TWCA CYBER Root CA OU = Root CA O = TAIWAN-CA C = TW
	Key Related Information
	Subject Public Key: RSA(4096 bits) Subject Key Identifiers: 9d 85 61 14 7c c1 62 6f 97 68 e4 4f 37 40 e1 ad e0 0d 56 37 Basic Constraint: Subject Type=CA Path Length Constraint= None Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)

2

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 400134B04F0000000000000004AA7B0A Signature Algorithm: sha384RSA Not Before: 2023-Feb-23 15:27:25 Not After: 2033-Feb-23 23:59:59 Thumbprint Algorithm: sha1 Thumbprint C9D8637AF4E4AC31E15AC44781CEE2E3E4D969AC Thumbprint Algorithm: sha2 Thumbprint F76E3339A6773DC5922DA154628C8D22B5C915EDCB15270DB8FB3D8D24959E98
	Issuer
	CN = TWCA CYBER Root CA OU = Root CA O = TAIWAN-CA C = TW
	Key Related Information
	Subject Public Key: RSA(4096 bits) Subject Key Identifiers: eb 82 76 72 51 b9 95 50 83 85 76 12 7f 83 18 f5 10 ec 10 53 Basic Constraint: Subject Type=CA Path Length Constraint=0 Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)

3

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) Basic Constraint: Subject Type=CA Path Length Constraint=None Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)

4

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)

5

TWCA CYBER Root CA	TWCA CYBER Root CA(Cross)
	Subject
	CN = TWCA CYBER Root CA OU = Root CA O =TAIWAN-CA C = TW
	Certificate Related Information
	Serial Number 4001348d190000000000000ccdf9937a Signature Algorithm: sha384RSA Not Before: 2022-Dec-9 12:00:27 Not After: 2030- Dec-9 23:59:59 Thumbprint Algorithm: sha1 Thumbprint 0f49cce5f4afb4701468954fdfb4357a4b6929fb Thumbprint Algorithm: sha2 Thumbprint C619F4E6F7B1BAA7A6C6F244092A3F82E46A6D67BEE26337FBAF02546F33133F
	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: 9d 85 61 14 7c c1 62 6f 97 68 e4 4f 37 40 e1 ad e0 0d 56 37 Basic Constraint: Subject Type=CA Path Length Constraint= None Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)

6

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: 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)

7

TWCA Global Root CA G2	TWCA Global Root CA G2(Cross)
	Subject
	CN = TWCA Global Root CA G2 OU = Root CA O = TAIWAN-CA C = TW
	Certificate Related Information
	Serial Number 4001348d190000000000000ccce78f26 Signature Algorithm: sha384RSA Not Before: 2022-Dec-9 11:44:17 Not After: 2030- Dec-9 23:59:59 Thumbprint Algorithm: sha1 Thumbprint 27ce93669629b5e45a61122addcf7a9cae2936a9 Thumbprint Algorithm: sha2 Thumbprint D53BF4968A7DB3C8C4E3366F2C7F76AD61B7041DFEFC64C1902C499A6FFFF241
	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: 92 8c d4 36 d1 5b 47 53 c4 71 0d 84 dd 64 2a f5 36 64 40 e7 Basic Constraint: Subject Type=CA Path Length Constraint= None Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)

8

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)

9

TWCA Global Root CA	TWCA Global Root CA(Cross)
	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-Oct-28 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)

10

TWCA EVSSL Certification Authority	TWCA EVSSL Certification Authority
	Subject
	CN=TWCA EVSSL Certification Authority O=TAIWAN-CA C=TW
	Certificate Related Information
	Serial Number 400134da0a00000000000000782d7a0 Signature Algorithm: sha384RSA Not Before: 2024-Sep-6 16:16:46 Not After: 2034-Sep-6 23:59:59 Thumbprint Algorithm: sha1 Thumbprint 92e92b121414b8c04248970fa62596aa138a81cc Thumbprint Algorithm: sha2 Thumbprint CAC9FD0CD35AA5C480CD03FDD6EDF0CA1A41FD02AC290EC83D83CEEDF8EC245C
	Issuer
	CN=TWCA CYBER Root CA OU=Root CA O=TAIWAN-CA C=TW
	Key Related Information
	Subject Public Key: RSA(4096 bits) Authority Key Identifiers: 9d 85 61 14 7c c1 62 6f 97 68 e4 4f 37 40 e1 ad e0 0d 56 37 Subject Key Identifiers: 5b 3c ba 2c da 44 dd eb 5c 4e 3d ce ee 58 f8 2e 55 92 1b 7a Basic Constraint: Subject Type=CA Path Length Constraint=0 Key Usage: Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)

11

TWCA Secure SSL Certification Authority	TWCA Secure SSL Certification Authority
	Subject
	CN = TWCA Secure SSL Certification Authority O = TAIWAN-CA C = TW
	Certificate Related Information
	Serial Number 400134b3680000000000000cd0aa08ec Signature Algorithm: sha256RSA Not Before: 2023-Oct-16 17:01:04 Not After: 2030-Oct-16 23:59:59 Thumbprint Algorithm: sha1 Thumbprint 7723f095467ebbe467cbe4a7db213975cf93c8b7 Thumbprint Algorithm: sha2 Thumbprint 1A2C75FD096E0499E9FF6AC74E526F61EAAE3EDFC8C2EA4436FEE0C24D8B7D0E
	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: 92 e7 fa 62 16 71 8c f3 97 71 42 c6 06 a7 e0 46 61 4b 5c b6 Basic Constraint: Subject Type=CA Path Length Constraint=0 Key Usage: Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)

12

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 400134b2a20000000000000ccf71354c Signature Algorithm: sha256RSA Not Before: 2023-Aug-18 11:14:13 Not After: 2030-Aug-18 23:59:59 Thumbprint Algorithm: sha1 Thumbprint 5c5cc99f05288ef78329895637b61db3b9b49815 Thumbprint Algorithm: sha2 Thumbprint C6E96A1745707099F02279472FA28A99BAE447D77511E19E86BAF3047651C1EB
	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: a0 92 06 71 0a b1 4a 50 0d 4f dc cf 19 c6 ad 13 cd 52 95 7b Basic Constraint: Subject Type=CA Path Length Constraint=0 Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)

13

TWCA SSL Certification Authority	TWCA SSL Certification Authority
	Subject
	CN = TWCA SSL Certification Authority O = TAIWAN-CA C = TW
	Certificate Related Information
	Serial Number 400134da0a0000000000000006aac553 Signature Algorithm: sha384RSA Not Before: 2024-Sep-6 15:48:36 Not After: 2034-Sep-6 23:59:59 Thumbprint Algorithm: sha1 Thumbprint 40b2cb275a144f620a4765a0eb1118ad9bcb704f Thumbprint Algorithm: sha2 Thumbprint 815C549C6976BF163EB54710FFC7806B1E7541C688313312B606837767164094
	Issuer
	CN = TWCA CYBER Root CA OU = Root CA O = TAIWAN-CA C = TW
	Key Related Information
	Subject Public Key: RSA(4096 bits) Authority Key Identifiers: 9d 85 61 14 7c c1 62 6f 97 68 e4 4f 37 40 e1 ad e0 0d 56 37 Subject Key Identifiers: 44 31 ab 0b 56 aa 48 61 bc fc 2f 09 24 51 bb cb ab d7 8a d9 Basic Constraint: Subject Type=CA Path Length Constraint=0 Key Usage: Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)

14

TWCA SSL Certification Authority	TWCA SSL Certification Authority
	Subject
	CN = TWCA SSL Certification Authority OU = SSL Sub-CA O =TAIWAN-CA C = TW
	Certificate Related Information
	Serial Number 400134B04F0000000000000003E324AC Signature Algorithm: sha384RSA Not Before: 2023-Feb-23 15:22:24 Not After: 2033-Feb-23 23:59:59 Thumbprint Algorithm: sha1 Thumbprint 1368673DF931FD2282E0AF472DBE0FF3FF8BE2B8 Thumbprint Algorithm: sha2 Thumbprint 01AF2324D098098F5E0CDF6FAABADA430B21CCE777F47EACB26248B2FDA3E531
	Issuer
	CN = TWCA CYBER Root CA OU = Root CA O = TAIWAN-CA C = TW
	Key Related Information
	Subject Public Key: RSA(4096 bits) Subject Key Identifiers: f2 28 d4 f9 d4 1c 7e 1a 6b 16 82 e5 ef 93 29 69 ed ca 15 20 Basic Constraint: Subject Type=CA Path Length Constraint=0 Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)

15

TWCA Global Root CA G2	TWCA Global Root CA G2
	Subject
	CN = TWCA Global Root CA G2 OU = Root CA O = TAIWAN-CA C = TW
	Certificate Related Information
	Serial Number 4001348cc2000000000000000019758f4 Signature Algorithm: sha384RSA Not Before: 2022-Nov-22 14:42:21 Not After: 2047- Nov-22 23:59:59 Thumbprint Algorithm: sha1 Thumbprint 73fe922f836391ffc8c6c4dad6202f6b072e7f1b Thumbprint Algorithm: sha2 Thumbprint 3A0072D49FFC04E996C59AEB75991D3C340F3615D6FD4DCE90AC0B3D88EAD4F4
	Issuer
	CN = TWCA Global Root CA G2 OU = Root CA O = TAIWAN-CA C = TW
	Key Related Information
	Subject Public Key: RSA(4096 bits) Subject Key Identifiers: 92 8c d4 36 d1 5b 47 53 c4 71 0d 84 dd 64 2a f5 36 64 40 e7 Basic Constraint: Subject Type=CA Path Length Constraint= None 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 12 years
Member A	Manager	PMP,CC, ISO 27001 LA	More then 8 years	More then 7 years
Member B	Assistant Manager	CC, ISO 27001 LA	More then 8 years	More then 7 years
Member C	Senior Consultant	CC, ISO 27001 LA	More then 7 years	More then 6 years
Member D	Consultant	CC, ISO 27001 LA	More then 5 years	More then 4 years

Appendix D – Publicly disclosed incidents

NO	Subject	Publicly Link
1	TWCA: TLS EV certificates with invalid subject attribute order	https://bugzilla.mozilla.org/show_bug.cgi?id=1883620
2	TWCA: Revocation delay for EV TLS certificates with invalid subject attribute order	https://bugzilla.mozilla.org/show_bug.cgi?id=1884568
3	TWCA: TLS certificates with non-critical basicConstraints	https://bugzilla.mozilla.org/show_bug.cgi?id=1885132
4	TWCA: Revocation delay for TLS certificates with non-critical basicConstraints	https://bugzilla.mozilla.org/show_bug.cgi?id=1886110

Assertion of Management as to
its Design of its Business Practices and its Controls Over
its Certification Authority Operations during the period
from January 1, 2024 through December 31, 2024

February 26, 2025

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

The management of TWCA is responsible for establishing and maintaining effective controls over its SSL CA operations, including its SSL CA business practices disclosure on its website SSL key lifecycle management controls, and SSL 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 SSL CA services. Based on that assessment, in providing its SSL Certification Authority services at Taipei city , New Taipei city and Taichung city, Taiwan, throughout the period January 1, 2024 to December 31, 2024, TWCA has:,

- disclosed its SSL certificate lifecycle management business practices in its:
  - TWCA Cyber Certification Authority Certification Practice Statement V1.1, effective from 29 February 2024; and
  - TWCA Public Key Infrastructure Certificate Policy V2.6.1, effective from 1 July 2024;

  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

in accordance with the WebTrust Principles and Criteria for Certification Authorities –SSL Baseline V2.8.

Title: President

Signature

Date February 26, 2025 CHAO-HUANG KUO

TAIWAN-CA INC. (TWCA)

10F., No.85, Yanping S. Rd., Zhongzheng Dist., Taipei City 100, Taiwan (R.O.C.)

Appendix – List of Root and Subordinate CAs in Scope

1

TWCA CYBER Root CA	TWCA CYBER Root CA
	Subject
	CN = TWCA CYBER Root CA OU = Root CA O =TAIWAN-CA C = TW
	Certificate Related Information
	Serial Number 4001348cc200000000000000013cf2c6 Signature Algorithm: sha384RSA Not Before: 2022-Nov-22 14:54:29 Not After: 2047- Nov-22 23:59:59 Thumbprint Algorithm: sha1 Thumbprint f6b11c1a8338e97bdbb3a8c83324e02d9c7f2666 Thumbprint Algorithm: sha2 Thumbprint 3F63BB2814BE174EC8B6439CF08D6D56F0B7C405883A5648A334424D6B3EC558
	Issuer
	CN = TWCA CYBER Root CA OU = Root CA O = TAIWAN-CA C = TW
	Key Related Information
	Subject Public Key: RSA(4096 bits) Subject Key Identifiers: 9d 85 61 14 7c c1 62 6f 97 68 e4 4f 37 40 e1 ad e0 0d 56 37 Basic Constraint: Subject Type=CA Path Length Constraint= None Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)

2

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 400134B04F0000000000000004AA7B0A Signature Algorithm: sha384RSA Not Before: 2023-Feb-23 15:27:25 Not After: 2033-Feb-23 23:59:59 Thumbprint Algorithm: sha1 Thumbprint C9D8637AF4E4AC31E15AC44781CEE2E3E4D969AC Thumbprint Algorithm: sha2 Thumbprint F76E3339A6773DC5922DA154628C8D22B5C915EDCB15270DB8FB3D8D24959E98
	Issuer
	CN = TWCA CYBER Root CA OU = Root CA O = TAIWAN-CA C = TW
	Key Related Information
	Subject Public Key: RSA(4096 bits) Subject Key Identifiers: eb 82 76 72 51 b9 95 50 83 85 76 12 7f 83 18 f5 10 ec 10 53 Basic Constraint: Subject Type=CA Path Length Constraint=0 Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)

3

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) Basic Constraint: Subject Type=CA Path Length Constraint=None Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)

4

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)

5

TWCA CYBER Root CA	TWCA CYBER Root CA(Cross)
	Subject
	CN = TWCA CYBER Root CA OU = Root CA O =TAIWAN-CA C = TW
	Certificate Related Information
	Serial Number 4001348d190000000000000ccdf9937a Signature Algorithm: sha384RSA Not Before: 2022-Dec-9 12:00:27 Not After: 2030- Dec-9 23:59:59 Thumbprint Algorithm: sha1 Thumbprint 0f49cce5f4afb4701468954fdfb4357a4b6929fb Thumbprint Algorithm: sha2 Thumbprint C619F4E6F7B1BAA7A6C6F244092A3F82E46A6D67BEE26337FBAF02546F33133F
	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: 9d 85 61 14 7c c1 62 6f 97 68 e4 4f 37 40 e1 ad e0 0d 56 37 Basic Constraint: Subject Type=CA Path Length Constraint= None Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)

6

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: 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)

7

TWCA Global Root CA G2	TWCA Global Root CA G2(Cross)
	Subject
	CN = TWCA Global Root CA G2 OU = Root CA O = TAIWAN-CA C = TW
	Certificate Related Information
	Serial Number 4001348d190000000000000ccce78f26 Signature Algorithm: sha384RSA Not Before: 2022-Dec-9 11:44:17 Not After: 2030- Dec-9 23:59:59 Thumbprint Algorithm: sha1 Thumbprint 27ce93669629b5e45a61122addcf7a9cae2936a9 Thumbprint Algorithm: sha2 Thumbprint D53BF4968A7DB3C8C4E3366F2C7F76AD61B7041DFEFC64C1902C499A6FFFF241
	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: 92 8c d4 36 d1 5b 47 53 c4 71 0d 84 dd 64 2a f5 36 64 40 e7 Basic Constraint: Subject Type=CA Path Length Constraint= None Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)

8

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)

9

TWCA Global Root CA	TWCA Global Root CA(Cross)
	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-Oct-28 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)

10

TWCA EVSSL Certification Authority	TWCA EVSSL Certification Authority
	Subject
	CN=TWCA EVSSL Certification Authority O=TAIWAN-CA C=TW
	Certificate Related Information
	Serial Number 400134da0a00000000000000782d7a0 Signature Algorithm: sha384RSA Not Before: 2024-Sep-6 16:16:46 Not After: 2034-Sep-6 23:59:59 Thumbprint Algorithm: sha1 Thumbprint 92e92b121414b8c04248970fa62596aa138a81cc Thumbprint Algorithm: sha2 Thumbprint CAC9FD0CD35AA5C480CD03FDD6EDF0CA1A41FD02AC290EC83D83CEEDF8EC245C
	Issuer
	CN=TWCA CYBER Root CA OU=Root CA O=TAIWAN-CA C=TW
	Key Related Information
	Subject Public Key: RSA(4096 bits) Authority Key Identifiers: 9d 85 61 14 7c c1 62 6f 97 68 e4 4f 37 40 e1 ad e0 0d 56 37 Subject Key Identifiers: 5b 3c ba 2c da 44 dd eb 5c 4e 3d ce ee 58 f8 2e 55 92 1b 7a Basic Constraint: Subject Type=CA Path Length Constraint=0 Key Usage: Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)

11

TWCA Secure SSL Certification Authority	TWCA Secure SSL Certification Authority
	Subject
	CN = TWCA Secure SSL Certification Authority O = TAIWAN-CA C = TW
	Certificate Related Information
	Serial Number 400134b3680000000000000cd0aa08ec Signature Algorithm: sha256RSA Not Before: 2023-Oct-16 17:01:04 Not After: 2030-Oct-16 23:59:59 Thumbprint Algorithm: sha1 Thumbprint 7723f095467ebbe467cbe4a7db213975cf93c8b7 Thumbprint Algorithm: sha2 Thumbprint 1A2C75FD096E0499E9FF6AC74E526F61EAAE3EDFC8C2EA4436FEE0C24D8B7D0E
	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: 92 e7 fa 62 16 71 8c f3 97 71 42 c6 06 a7 e0 46 61 4b 5c b6 Basic Constraint: Subject Type=CA Path Length Constraint=0 Key Usage: Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)

12

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 400134b2a20000000000000ccf71354c Signature Algorithm: sha256RSA Not Before: 2023-Aug-18 11:14:13 Not After: 2030-Aug-18 23:59:59 Thumbprint Algorithm: sha1 Thumbprint 5c5cc99f05288ef78329895637b61db3b9b49815 Thumbprint Algorithm: sha2 Thumbprint C6E96A1745707099F02279472FA28A99BAE447D77511E19E86BAF3047651C1EB
	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: a0 92 06 71 0a b1 4a 50 0d 4f dc cf 19 c6 ad 13 cd 52 95 7b Basic Constraint: Subject Type=CA Path Length Constraint=0 Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)

13

TWCA SSL Certification Authority	TWCA SSL Certification Authority
	Subject
	CN = TWCA SSL Certification Authority O = TAIWAN-CA C = TW
	Certificate Related Information
	Serial Number 400134da0a0000000000000006aac553 Signature Algorithm: sha384RSA Not Before: 2024-Sep-6 15:48:36 Not After: 2034-Sep-6 23:59:59 Thumbprint Algorithm: sha1 Thumbprint 40b2cb275a144f620a4765a0eb1118ad9bcb704f Thumbprint Algorithm: sha2 Thumbprint 815C549C6976BF163EB54710FFC7806B1E7541C688313312B606837767164094
	Issuer
	CN = TWCA CYBER Root CA OU = Root CA O = TAIWAN-CA C = TW
	Key Related Information
	Subject Public Key: RSA(4096 bits) Authority Key Identifiers: 9d 85 61 14 7c c1 62 6f 97 68 e4 4f 37 40 e1 ad e0 0d 56 37 Subject Key Identifiers: 44 31 ab 0b 56 aa 48 61 bc fc 2f 09 24 51 bb cb ab d7 8a d9 Basic Constraint: Subject Type=CA Path Length Constraint=0 Key Usage: Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)

14

TWCA SSL Certification Authority	TWCA SSL Certification Authority
	Subject
	CN = TWCA SSL Certification Authority OU = SSL Sub-CA O =TAIWAN-CA C = TW
	Certificate Related Information
	Serial Number 400134B04F0000000000000003E324AC Signature Algorithm: sha384RSA Not Before: 2023-Feb-23 15:22:24 Not After: 2033-Feb-23 23:59:59 Thumbprint Algorithm: sha1 Thumbprint 1368673DF931FD2282E0AF472DBE0FF3FF8BE2B8 Thumbprint Algorithm: sha2 Thumbprint 01AF2324D098098F5E0CDF6FAABADA430B21CCE777F47EACB26248B2FDA3E531
	Issuer
	CN = TWCA CYBER Root CA OU = Root CA O = TAIWAN-CA C = TW
	Key Related Information
	Subject Public Key: RSA(4096 bits) Subject Key Identifiers: f2 28 d4 f9 d4 1c 7e 1a 6b 16 82 e5 ef 93 29 69 ed ca 15 20 Basic Constraint: Subject Type=CA Path Length Constraint=0 Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)

15

TWCA Global Root CA G2	TWCA Global Root CA G2
	Subject
	CN = TWCA Global Root CA G2 OU = Root CA O = TAIWAN-CA C = TW
	Certificate Related Information
	Serial Number 4001348cc2000000000000000019758f4 Signature Algorithm: sha384RSA Not Before: 2022-Nov-22 14:42:21 Not After: 2047- Nov-22 23:59:59 Thumbprint Algorithm: sha1 Thumbprint 73fe922f836391ffc8c6c4dad6202f6b072e7f1b Thumbprint Algorithm: sha2 Thumbprint 3A0072D49FFC04E996C59AEB75991D3C340F3615D6FD4DCE90AC0B3D88EAD4F4
	Issuer
	CN = TWCA Global Root CA G2 OU = Root CA O = TAIWAN-CA C = TW
	Key Related Information
	Subject Public Key: RSA(4096 bits) Subject Key Identifiers: 92 8c d4 36 d1 5b 47 53 c4 71 0d 84 dd 64 2a f5 36 64 40 e7 Basic Constraint: Subject Type=CA Path Length Constraint= None Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)