



## 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 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 V1.3; and
  - TWCA Global Certification Authority Certification Practice Statement V1.4.1(draft, Effective from June 20, 2019); 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 V2.4.1.

### **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 V2.4.1.



## **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.

## **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, 2019 to December 31, 2019, 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 V2.4.1.

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 – SSL Baseline with Network Security V2.4.1, 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 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.

A handwritten signature of the KPMG logo in black ink.

KPMG

Certified Public Accountants

Taipei, Taiwan, ROC

February 24, 2020



Appendix A – List of Root and Subordinate CAs in Scope

| TWCA Global Root CA   |   |
|---|---|
| Subject   | Issuer  |
| CN = TWCA Global Root CA<br>OU = Root CA<br>O = TAIWAN-CA<br>C = TW   | CN = TWCA Global Root CA<br>OU = Root CA<br>O = TAIWAN-CA<br>C = TW |
| Certificate Related Information   | Key Related Information   |
| Serial Number 0cbe<br>Signature Algorithm: sha256RSA<br>Not Before: 2012-Jun-27 14:28:33<br>Not After: 2030-Dec-31 23:59:59<br>Thumbprint Algorithm: sha1<br>Thumbprint<br>9cbb4853f6a4f6d352a4e832525560<br>13f5adaf65 | Subject Public Key: RSA(4096 bits)<br>Subject Key Identifiers:      |

| TWCA Root Certification Authority   |  |
|---|--|
| Subject   | Issuer   |
| CN = TWCA Root Certification Authority<br>OU = Root CA<br>O = TAIWAN-CA<br>C = TW   | CN = TWCA Root Certification Authority<br>OU = Root CA<br>O = TAIWAN-CA<br>C = TW  |
| Certificate Related Information   | Key Related Information  |
| Serial Number 01<br>Signature Algorithm: sha256RSA<br>Not Before: 2008-Aug-28 03:47:13<br>Not After: 2030-Dec-31 23:59:59<br>Thumbprint Algorithm: sha1<br>Thumbprint<br>df646dcb7b0fd3a96aee88c64e2d67<br>6711ff9d5f | Subject Public Key: RSA(4096 bits)<br>Subject Key Identifiers: c8 44 5a fe 7f fd a9 9b 86 35 be e2 a5 f6 19 fb 5e bf 6f 59<br>Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06) |



| TWCA Root Certification Authority(2048)   |  |
|---|--|
| Subject   | Issuer   |
| CN = TWCA Root Certification Authority<br>OU = Root CA<br>O = TAIWAN-CA<br>C = TW   | CN = TWCA Root Certification Authority<br>OU = Root CA<br>O = TAIWAN-CA<br>C = TW  |
| Certificate Related Information   | Key Related Information  |
| Serial Number 01<br>Signature Algorithm: sha1RSA<br>Not Before: 2008-Aug-28 15:24:33<br>Not After: 2030-Dec-31 23:59:59<br>Thumbprint Algorithm: sha1<br>Thumbprint<br>cf9e876dd3ebfc422697a3b5a37aa0<br>76a9062348 | Subject Public Key: RSA(2048 bits)<br>Subject Key Identifiers: 6a 38 5b 26 8d de 8b 5a f2 4f 7a 54 83 19 18 e3 08 35 a6 ba<br>Basic Constraint: Subject Type=CA<br>Path Length Constraint=None<br>Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06) |

| TWCA Global Root CA(4096)  |  |
|--|--|
| Subject  | Issuer   |
| CN = TWCA Global Root CA<br>OU = Root CA<br>O = TAIWAN-CA<br>C = TW  | CN = TWCA Root Certification Authority<br>OU = Root CA<br>O = TAIWAN-CA<br>C = TW  |
| Certificate Related Information  | Key Related Information  |
| Serial Number<br>40013353e4000000000000cca5d<br>1b69<br>Signature Algorithm: sha256RSA<br>Not Before: 2014-Oct-28<br>15:38:31<br>Not After: 2030-Dec-31 23:59:59<br>Thumbprint Algorithm: sha1<br>Thumbprint<br>fd54e4643b49705a2aaae50653c4f<br>56c2df8083d | Subject Public Key: RSA(2048 bits)<br>Subject Key Identifiers: 6a 38 5b 26 8d de 8b 5a f2 4f 7a 54 83 19 18 e3 08 35 a6 ba<br>Basic Constraint: Subject Type=CA<br>Path Length Constraint=None<br>Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06) |



| TWCA Secure SSL Certification Authority   |   |
|---|---|
| Subject   | Issuer  |
| CN = TWCA Secure SSL Certification Authority<br>OU = Secure SSL Sub-CA<br>O = TAIWAN-CA<br>C = TW   | CN = TWCA Global Root CA<br>OU = Root CA<br>O = TAIWAN-CA<br>C = TW   |
| Certificate Related Information   | Key Related Information   |
| Serial Number<br>40013353e400000000000000cc36e888d<br>Signature Algorithm: sha256RSA<br>Not Before: 2014-Oct-28 15:27:56<br>Not After: 2024-Oct-28 23:59:59<br>Thumbprint Algorithm: sha1<br>Thumbprint<br>0a72efd660fd34f254e66a8595ba81e60a754e68 | Subject Public Key: RSA(2048 bits)<br>Authority Key Identifiers: 48 db cd de 8e e9 49 72 5a 88 e8 b1 d8 3d 07 b3 b9 6b 66 50<br>Subject Key Identifiers: f8 07 c2 68 24 ff 85 95 cb db 1e e3 33 9c 2a 4f 97 20 56 7b<br>Basic Constraint: Subject Type=CA<br>Path Length Constraint=0<br>Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06) |

| TWCA Global EVSSL Certification Authority   |   |
|---|---|
| Subject   | Issuer  |
| CN = TWCA Global EVSSL Certification Authority<br>OU = Global EVSSL Sub-CA<br>O = TAIWAN-CA<br>C = TW   | CN = TWCA Global Root CA<br>OU = Root CA<br>O = TAIWAN-CA<br>C = TW   |
| Certificate Related Information   | Key Related Information   |
| Serial Number<br>40013304f700000000000000cc042cd6d<br>Signature Algorithm: sha256RSA<br>Not Before: 2012-Aug-23 17:53:30<br>Not After: 2030-Aug-23 23:59:59<br>Thumbprint Algorithm: sha1<br>Thumbprint<br>071a25fa76a200da3c53f1ee791e7b627d32c349 | Subject Public Key:RSA(2048 bits)<br>Authority Key Identifiers: 48 db cd de 8e e9 49 72 5a 88 e8 b1 d8 3d 07 b3 b9 6b 66 50<br>Subject Key Identifiers: e4 6e bd a1 2b ce e4 c2 d5 28 74 5c bd d9 8c 6f 04 72 2a 06 de<br>Basic Constraint: Subject Type=CA<br>Path Length Constraint=0<br>Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06) |





| TWCA EVSSL Certification Authority  |  |
|---|--|
| Subject   | Issuer   |
| CN = TWCA EVSSL Certification Authority<br>OU = EVSSL Sub-CA<br>O = TAIWAN-CA<br>C = TW   | CN = TWCA Root Certification Authority<br>OU = Root CA<br>O = TAIWAN-CA<br>C = TW  |
| Certificate Related Information   | Key Related Information  |
| Serial Number<br>400132dd12000000000000cc1e1f977<br>Signature Algorithm: sha1RSA<br>Not Before: 2011-Jun-10 10:49:38<br>Not After: 2021-Jun-10 23:59:59<br>Thumbprint Algorithm: sha1<br>Thumbprint<br>29429d028287a76c6c236e195e237e2407cd291d | Subject Public Key: RSA(2048 bits)<br>Authority Key Identifiers: 6a 38 5b 26 8d de 8b 5a f2 4f 7a 54 83 19 18 e3 08 35 a6 ba<br>Subject Key Identifiers: b9 2c 09 b5 34 2a f9 fe 5c 0d fd 6f 76 8b d5 92 1a e4 61 56<br>Basic Constraint: Subject Type=CA Path Length Constraint=0<br>Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06) |

| TWCA InfoSec User CA  |   |
|---|---|
| Subject   | Issuer  |
| CN = TWCA InfoSec User CA<br>OU = User CA<br>O = TAIWAN-CA Inc.<br>C = TW   | CN = TWCA Root Certification Authority<br>OU = Root CA<br>O = TAIWAN-CA<br>C = TW   |
| Certificate Related Information   | Key Related Information   |
| Serial Number<br>4001330420000000000000cc2901d53<br>Signature Algorithm: sha1RSA<br>Not Before: 2012-Jun-8 09:51:19<br>Not After: 2022-Jun-8 23:59:59<br>Thumbprint Algorithm: sha1<br>Thumbprint<br>a25d976f92d89c9cdd6f57b1b80b51f56e0042f9 | Subject Public Key: RSA(2048 bits)<br>Authority Key Identifiers: =6a 38 5b 26 8d de 8b 5a f2 4f 7a 54 83 19 18 e3 08 35 a6 ba<br>Subject Key Identifiers: 21 20 6a 92 e9 69 5b ac c8 63 eb 64 ce 82 c1 51 66 2a 87 e2<br>Basic Constraint: Subject Type=CA Path Length Constraint=0<br>Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06) |



| Subordinate CA Certificate   |  |
|--|--|
| Subject  | Issuer   |
| CN = TWCA InfoSec User CA<br>OU = User CA<br>O = TAIWAN-CA Inc.<br>C = TW  | CN = TWCA Root Certification Authority<br>OU = Root CA<br>O = TAIWAN-CA<br>C = TW  |
| Certificate Related Information  | Key Related Information  |
| Serial Number<br>40013353e400000000000000cc97138a0<br>Signature Algorithm: sha256RSA<br>Not Before: 2014-Oct-28 02:48:11<br>Not After: 2024-Oct-28 23:59:59<br>Thumbprint Algorithm: sha1<br>Thumbprint<br>58e9110cd66036337f7e0d46cbb94587fae0e19 | Subject Public Key: RSA(2048 bits)<br>Authority Key Identifiers: 6a 38 5b 26 8d de 8b 5a f2 4f 7a 54 83 19 18 e3 08 35 a6 ba<br>Subject Key Identifiers: d9 10 f0 de c2 a1 99 f5 7e 4b 93 a2 13 c6 d6 46 73 c2 49 de<br>Basic Constraint: Subject Type=CA Path Length Constraint=0<br>Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06) |

| TWCA InfoSec User CA  |  |
|---|--|
| Subject   | Issuer   |
| CN = TWCA InfoSec User CA<br>OU = User CA<br>O = TAIWAN-CA Inc.<br>C = TW   | CN = TWCA Root Certification Authority<br>OU = Root CA<br>O = TAIWAN-CA<br>C = TW  |
| Certificate Related Information   | Key Related Information  |
| Serial Number<br>400133f01400000000000000ccfae3cd7<br>Signature Algorithm: sha1RSA<br>Not Before: 2018-Oct-12 11:03:57<br>Not After: 2028-Oct-12 23:59:59<br>Thumbprint Algorithm: sha1<br>Thumbprint<br>910a43afdd86271f30dd937ee6ad92b1324434d2 | Subject Public Key: RSA(2048 bits)<br>Authority Key Identifiers: 6a 38 5b 26 8d de 8b 5a f2 4f 7a 54 83 19 18 e3 08 35 a6 ba<br>Subject Key Identifiers: 46 6f 16 86 f4 a0 5b 11 41 be 93 6a ec 06 50 ce 8a 55 46 59<br>Basic Constraint: Subject Type=CA Path Length Constraint=0<br>Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06) |



| TWCA InfoSec User CA       |  |   |
|----------------------------|--|---|
|                            | Subject  | Issuer  |
| TWCA<br>InfoSec<br>User CA | CN = TWCA InfoSec User CA<br>OU = User CA<br>O = TAIWAN-CA Inc.<br>C = TW  | CN = TWCA Global Root CA<br>OU = Root CA<br>O = TAIWAN-CA<br>C = TW   |
|                            | Certificate Related Information  | Key Related Information   |
|                            | Serial Number<br>400133f01400000000000000cc7024<br>1af<br>Signature Algorithm: sha256RSA<br>Not Before: 2018-Oct-12 04:45:27<br>Not After: 2028- Oct-12 23:59:59<br>Thumbprint Algorithm: sha256<br>Thumbprint<br>5bbe8e290dab5c984c154500dd163<br>79cb2704d20 | Subject Public Key: RSA(2048 bits)<br>Authority Key Identifiers: 48 db cd de 8e e9 49 72 5a 88 e8 b1 d8 3d 07 b3 b9 6b 66 50<br>Subject Key Identifiers: 1a 7c e5 e7 6a 1f 61 8e 4b aa b6 fc fb f6 90 85 ee 84 09 fe<br>Basic Constraint: Subject Type=CA<br>Path Length Constraint=0<br>Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06) |
|                            |  |   |