



## 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](#), TWCA has:

- disclosed its extended validation 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 EV SSL certificates in conformity with the CA/Browser Forum Guidelines 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 EV SSL certificates it manages is established and protected throughout their lifecycles; and



- EV SSL subscriber information is properly authenticated for the registration activities performed by TWCA

in accordance with the [WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL Version v1.8.](#)

In addition , we have examined and found no evidence that Secure SSL CA had issued any EVSSL certificates throughout the period January 1, 2024 to December 31, 2024.

### **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 - Extended Validation SSL Version 1.8.

### **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 EV SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of EV SSL certificates;
2. selectively testing transactions executed in accordance with disclosed EV 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 - Extended Validation SSL Version 1.8.

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 - Extended Validation SSL v1.8,



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

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



3

|                           |  |
|---------------------------|--|
| TWCA<br>Global Root<br>CA | TWCA Global Root CA  |
|                           | Subject  |
|                           | CN = TWCA Global Root CA<br>OU = Root CA<br>O = TAIWAN-CA<br>C = TW  |
|                           | Certificate 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 9cbb4853f6a4f6d352a4e83252556013f5adaf65<br>Thumbprint Algorithm: sha2<br>Thumbprint<br>59769007F7685D0FCD50872F9F95D5755A5B2B457D81F3692B610A98672F0E1B |
|                           | Issuer   |
|                           | CN = TWCA Global Root CA<br>OU = Root CA<br>O = TAIWAN-CA<br>C = TW  |
|                           | Key Related Information  |
|                           | Subject Public Key: RSA(4096 bits)<br>Basic Constraint: Subject Type=CA<br>Path Length Constraint=None<br>Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)   |
|                           |  |

|  |   |
|--|---|
| TWCA<br>Secure SSL<br>Certification<br>Authority | TWCA Secure SSL Certification Authority   |
|  | Subject   |
|  | CN = TWCA Secure SSL Certification Authority<br>OU = Secure SSL Sub-CA<br>O = TAIWAN-CA<br>C = TW   |
|  | Certificate Related Information   |
|  | Serial Number 40013353e4000000000000cc36e888d<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 0a72efd660fd34f254e66a8595ba81e60a754e68<br>Thumbprint Algorithm: sha2<br>Thumbprint<br>9B16F2F680D7C4BD6A67F609340DA6416ABF9E43F1326B01B988192271D0B5F2           |
|  | Issuer  |
|  | CN = TWCA Global Root CA<br>OU = Root CA<br>O = TAIWAN-CA<br>C = TW   |
|  | Key Related Information   |
|  | 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<br>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<br>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<br>CYBER<br>Root CA | TWCA CYBER Root CA(Cross)   |  |
|                          | Subject   |  |
|                          | CN = TWCA CYBER Root CA<br>OU = Root CA<br>O =TAIWAN-CA<br>C = TW   |  |
|                          | Certificate Related Information   |  |
|                          | Serial Number 4001348d1900000000000000ccdf9937a<br>Signature Algorithm: sha384RSA<br>Not Before: 2022-Dec-9 12:00:27<br>Not After: 2030- Dec-9 23:59:59<br>Thumbprint Algorithm: sha1<br>Thumbprint 0f49cce5f4afb4701468954fdb4357a4b6929fb<br>Thumbprint Algorithm: sha2<br>Thumbprint<br>C619F4E6F7B1BAA7A6C6F244092A3F82E46A6D67BEE26337FBAF02546F33133F |  |
|                          | Issuer  |  |
|                          | CN = TWCA Global Root CA<br>OU = Root CA<br>O = TAIWAN-CA<br>C = TW   |  |
|                          | Key Related Information   |  |
|                          | Subject Public Key: RSA(4096 bits)<br>Subject Key Identifiers: 9d 85 61 14 7c c1 62 6f 97 68 e4 4f 37 40 e1 ad e0 0d 56 37<br>Basic Constraint: Subject Type=CA<br>Path Length Constraint= None<br>Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)   |  |
|                          |   |  |
|                          |   |  |

|   |  |  |
|---|--|--|
| TWCA<br>Global<br>EVSSL<br>Certification<br>Authority | TWCA Global EVSSL Certification Authority  |  |
|   | Subject  |  |
|   | CN = TWCA Global EVSSL Certification Authority<br>OU = Global EVSSL Sub-CA<br>O = TAIWAN-CA<br>C = TW  |  |
|   | Certificate Related Information  |  |
|   | Serial Number 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 071a25fa76a200da3c53f1ee791e7b627d32c349<br>Thumbprint Algorithm: sha2<br>Thumbprint<br>49695A5F0F7EF6EDF698193D99ED48BAADE20EA457403C11CEAD492C458665DA  |  |
|   | Issuer   |  |
|   | CN = TWCA Global Root CA<br>OU = Root CA<br>O = TAIWAN-CA<br>C = TW  |  |
|   | Key Related Information  |  |
|   | 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: 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<br>Global Root<br>CA G2 | TWCA Global Root CA G2(Cross)   |  |
|                              | Subject   |  |
|                              | CN = TWCA Global Root CA G2<br>OU = Root CA<br>O = TAIWAN-CA<br>C = TW  |  |
|                              | Certificate Related Information   |  |
|                              | Serial Number 4001348d1900000000000000ccce78f26   |  |
|                              | 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<br>D53BF4968A7DB3C8C4E3366F2C7F76AD61B7041DFEFC64C1902C499A6FFFF241  |  |
|                              | Issuer  |  |
|                              | CN = TWCA Global Root CA<br>OU = Root CA<br>O = TAIWAN-CA<br>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<br>Path Length Constraint= None<br>Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06) |  |

|                                   |   |  |
|-----------------------------------|---|--|
| TWCA Root Certification Authority | TWCA Root Certification Authority(2048)   |  |
|                                   | Subject   |  |
|                                   | CN = TWCA Root Certification Authority<br>OU = Root CA<br>O = TAIWAN-CA<br>C = TW   |  |
|                                   | Certificate 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 cf9e876dd3ebfc422697a3b5a37aa076a9062348<br>Thumb print Algorithm: sha2<br>Thumbprint<br>BFD88FE1101C41AE3E801BF8BE56350EE9BAD1A6B9BD515EDC5C6D5B8711AC44 |  |
|                                   | Issuer  |  |
|                                   | CN = TWCA Root Certification Authority<br>OU = Root CA<br>O = TAIWAN-CA<br>C = TW   |  |
|                                   | Key Related Information   |  |
|                                   | 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<br>Global Root<br>CA | TWCA Global Root CA(Cross)  |  |
|                           | Subject   |  |
|                           | CN = TWCA Global Root CA<br>OU = Root CA<br>O = TAIWAN-CA<br>C = TW   |  |
|                           | Certificate Related Information   |  |
|                           | Serial Number: 40013353e40000000000000cca5d1b69<br>Signature Algorithm: sha256RSA<br>Not Before: 2014-Oct-28 15:38:31<br>Not After: 2030-Oct-28 23:59:59<br>Thumbprint Algorithm: sha1<br>Thumbprint fd54e4643b49705a2aaae50653c4f56c2df8083d<br>Thumbprint Algorithm: sha2<br>Thumbprint<br>8AD47F6D70A44FA80AF0F931125FFE3A76876FFAD219A4D40A13C038DC85E69E |  |
|                           | Issuer  |  |
|                           | CN = TWCA Root Certification Authority<br>OU = Root CA<br>O = TAIWAN-CA<br>C = TW   |  |
|                           | Key Related Information   |  |
|                           | Subject Public Key: RSA(4096 bits)<br>Subject Key Identifiers:<br>48 db cd de 8e e9 49 72 5a 88 e8 b1 d8 3d 07 b3 b9 6b 66 50<br>Basic Constraint: Subject Type=CA<br>Path Length Constraint=None<br>Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)   |  |
|                           |   |  |

|   |  |  |
|---|--|--|
| TWCA<br>EVSSL<br>Certification<br>Authority | TWCA EVSSL Certification Authority   |  |
|   | Subject  |  |
|   | CN=TWCA EVSSL Certification Authority<br>O=TAIWAN-CA<br>C=TW   |  |
|   | Certificate Related Information  |  |
|   | Serial Number 400134da0a0000000000000000782d7a0<br>Signature Algorithm: sha384RSA<br>Not Before: 2024-Sep-6 16:16:46<br>Not After: 2034-Sep-6 23:59:59<br>Thumbprint Algorithm: sha1<br>Thumbprint 92e92b121414b8c04248970fa62596aa138a81cc<br>Thumbprint Algorithm: sha2<br>Thumbprint<br>CAC9FD0CD35AA5C480CD03FDD6EDF0CA1A41FD02AC290EC83D83CEEDF8EC245C                        |  |
|   | Issuer   |  |
|   | CN=TWCA CYBER Root CA<br>OU=Root CA<br>O=TAIWAN-CA<br>C=TW   |  |
|   | Key Related Information  |  |
|   | Subject Public Key: RSA(4096 bits)<br>Authority Key Identifiers: 9d 85 61 14 7c c1 62 6f 97 68 e4 4f 37 40 e1 ad e0 0d 56 37<br>Subject Key Identifiers: 5b 3c ba 2c da 44 dd eb 5c 4e 3d ce ee 58 f8 2e 55 92 1b 7a<br>Basic Constraint: Subject Type=CA<br>Path Length Constraint=0<br>Key Usage: Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86) |  |
|   |  |  |



11

|                              |  |
|------------------------------|--|
| TWCA<br>Global Root<br>CA G2 | TWCA Global Root CA G2   |
|                              | <b>Subject</b>   |
|                              | CN = TWCA Global Root CA G2<br>OU = Root CA<br>O = TAIWAN-CA<br>C = TW   |
|                              | <b>Certificate Related Information</b>   |
|                              | Serial Number 4001348cc2000000000000000019758f4<br>Signature Algorithm: sha384RSA<br>Not Before: 2022-Nov-22 14:42:21<br>Not After: 2047- Nov-22 23:59:59<br>Thumbprint Algorithm: sha1<br>Thumbprint 73fe922f836391ffc8c6c4dad6202f6b072e7f1b<br>Thumbprint Algorithm: sha2<br>Thumbprint<br>3A0072D49FFC04E996C59AEB75991D3C340F3615D6FD4DCE90AC0B3D88EAD4F4 |
|                              | <b>Issuer</b>  |
|                              | CN = TWCA Global Root CA G2<br>OU = Root CA<br>O = TAIWAN-CA<br>C = TW   |
|                              | <b>Key Related Information</b>   |
|                              | Subject Public Key: RSA(4096 bits)<br>Subject Key Identifiers: 92 8c d4 36 d1 5b 47 53 c4 71 0d 84 dd 64 2a f5 36 64 40 e7<br>Basic Constraint: Subject Type=CA<br>Path Length Constraint= None<br>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 |
|--------------------|----------------------|---|-----------------------|------------------------------|
| <b>Team Leader</b> | Partner              | CISA,IRCA<br>Registered<br>ISO 27001 LA | More than<br>20 years | More than 12 years           |
| <b>Member A</b>    | Manager              | PMP,CC,<br>ISO 27001 LA                 | More then 8<br>years  | More then 7 years            |
| <b>Member B</b>    | Assistant<br>Manager | CC,<br>ISO 27001 LA                     | More then 8<br>years  | More then 7 years            |
| <b>Member C</b>    | Senior<br>Consultant | CC,<br>ISO 27001 LA                     | More then 7<br>years  | More then 6 years            |
| <b>Member D</b>    | Consultant           | CC,<br>ISO 27001 LA                     | More then 5<br>years  | More then 4 years            |

## Appendix D – Publicly disclosed incidents

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



**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 and TWCA EVSSL Certification Authority, and provides Extended Validation SSL (“EV 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 EV SSL CA operations, including its EV SSL CA business practices disclosure on its [website](#), EV SSL key lifecycle management controls, and EV 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 the disclosure of its certificate practice and controls over its EVSSL CA services. Based on that assessment, in TWCA Management's opinion, in providing its EV SSL CA services located at Taipei city , New Taipei city and Taichung city, Taiwan , throughout the period January 1, 2024 to December 31, 2024. TWCA EVSSL Certification Authority CA has:

- disclosed its extended validation SSL ("EV SSL") certificate lifecycle 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 EV SSL certificates in conformity with the CA/Browser Forum Guidelines 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 EV certificates it managed is established and protected throughout their life cycles; and
  - EV Subscriber information was properly authenticated (for the registration activities performed by TWCA)

in accordance with the [WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL Version v1.8.](#)

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

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



|                           |  |
|---------------------------|--|
| TWCA<br>Global Root<br>CA | <b>TWCA Global Root CA</b>   |
|                           | <b>Subject</b>   |
|                           | CN = TWCA Global Root CA<br>OU = Root CA<br>O = TAIWAN-CA<br>C = TW  |
|                           | <b>Certificate Related Information</b>   |
|                           | 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 9cbb4853f6a4f6d352a4e83252556013f5adaf65<br>Thumbprint Algorithm: sha2<br>Thumbprint<br>59769007F7685D0FCD50872F9F95D5755A5B2B457D81F3692B610A98672F0E1B |
|                           | <b>Issuer</b>  |
|                           | CN = TWCA Global Root CA<br>OU = Root CA<br>O = TAIWAN-CA<br>C = TW  |
|                           | <b>Key Related Information</b>   |
|                           | Subject Public Key: RSA(4096 bits)<br>Basic Constraint: Subject Type=CA<br>Path Length Constraint=None<br>Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)   |
|                           |  |

|  |   |  |
|--|---|--|
| TWCA<br>Secure SSL<br>Certification<br>Authority | TWCA Secure SSL Certification Authority   |  |
|  | Subject   |  |
|  | CN = TWCA Secure SSL Certification Authority<br>OU = Secure SSL Sub-CA<br>O = TAIWAN-CA<br>C = TW   |  |
|  | Certificate Related Information   |  |
|  | Serial Number 40013353e4000000000000cc36e888d<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 0a72efd660fd34f254e66a8595ba81e60a754e68<br>Thumbprint Algorithm: sha2<br>Thumbprint<br>9B16F2F680D7C4BD6A67F609340DA6416ABF9E43F1326B01B988192271D0B5F2           |  |
|  | Issuer  |  |
|  | CN = TWCA Global Root CA<br>OU = Root CA<br>O = TAIWAN-CA<br>C = TW   |  |
|  | Key Related Information   |  |
|  | 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<br>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<br>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<br>CYBER<br>Root CA | TWCA CYBER Root CA(Cross)   |  |
|                          | Subject   |  |
|                          | CN = TWCA CYBER Root CA<br>OU = Root CA<br>O =TAIWAN-CA<br>C = TW   |  |
|                          | Certificate Related Information   |  |
|                          | Serial Number 4001348d1900000000000000ccdf9937a<br>Signature Algorithm: sha384RSA<br>Not Before: 2022-Dec-9 12:00:27<br>Not After: 2030- Dec-9 23:59:59<br>Thumbprint Algorithm: sha1<br>Thumbprint 0f49cce5f4afb4701468954fdb4357a4b6929fb<br>Thumbprint Algorithm: sha2<br>Thumbprint<br>C619F4E6F7B1BAA7A6C6F244092A3F82E46A6D67BEE26337FBAF02546F33133F |  |
|                          | Issuer  |  |
|                          | CN = TWCA Global Root CA<br>OU = Root CA<br>O = TAIWAN-CA<br>C = TW   |  |
|                          | Key Related Information   |  |
|                          | Subject Public Key: RSA(4096 bits)<br>Subject Key Identifiers: 9d 85 61 14 7c c1 62 6f 97 68 e4 4f 37 40 e1 ad e0<br>0d 56 37<br>Basic Constraint: Subject Type=CA<br>Path Length Constraint= None<br>Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)  |  |
|                          |   |  |
|                          |   |  |

|   |  |  |
|---|--|--|
| TWCA<br>Global<br>EVSSL<br>Certification<br>Authority | TWCA Global EVSSL Certification Authority  |  |
|   | <b>Subject</b>   |  |
|   | CN = TWCA Global EVSSL Certification Authority<br>OU = Global EVSSL Sub-CA<br>O = TAIWAN-CA<br>C = TW  |  |
|   | <b>Certificate Related Information</b>   |  |
|   | Serial Number 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 071a25fa76a200da3c53f1ee791e7b627d32c349<br>Thumbprint Algorithm: sha2<br>Thumbprint<br>49695A5F0F7EF6EDF698193D99ED48BAADE20EA457403C11CEAD492C458665DA        |  |
|   | <b>Issuer</b>  |  |
|   | CN = TWCA Global Root CA<br>OU = Root CA<br>O = TAIWAN-CA<br>C = TW  |  |
|   | <b>Key Related Information</b>   |  |
|   | 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<br>b9 6b 66 50<br>Subject Key Identifiers: 6e bd a1 2b ce e4 c2 d5 28 74 5c bd d9 8c 6f 04 72<br>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<br>Global Root<br>CA G2 | TWCA Global Root CA G2(Cross)  |  |
|                              | <b>Subject</b>   |  |
|                              | CN = TWCA Global Root CA G2<br>OU = Root CA<br>O = TAIWAN-CA<br>C = TW               |  |
|                              | <b>Certificate Related Information</b>   |  |
|                              | Serial Number 4001348d1900000000000000ccce78f26                                      |  |
|                              | 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<br>D53BF4968A7DB3C8C4E3366F2C7F76AD61B7041DFEFC64C1902C499A6FFFF241       |  |
|                              | <b>Issuer</b>  |  |
|                              | CN = TWCA Global Root CA<br>OU = Root CA<br>O = TAIWAN-CA<br>C = TW                  |  |
|                              | <b>Key Related Information</b>   |  |
|                              | 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)               |  |

|  |   |  |
|--|---|--|
| TWCA<br>Root<br>Certification<br>Authority | TWCA Root Certification Authority(2048)   |  |
|  | <b>Subject</b>  |  |
|  | CN = TWCA Root Certification Authority<br>OU = Root CA<br>O = TAIWAN-CA<br>C = TW   |  |
|  | <b>Certificate Related Information</b>  |  |
|  | 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 cf9e876dd3ebfc422697a3b5a37aa076a9062348<br>Thumb print Algorithm: sha2<br>Thumbprint<br>BFD88FE1101C41AE3E801BF8BE56350EE9BAD1A6B9BD515EDC5C6D5B8711AC44 |  |
|  | <b>Issuer</b>   |  |
|  | CN = TWCA Root Certification Authority<br>OU = Root CA<br>O = TAIWAN-CA<br>C = TW   |  |
|  | <b>Key Related Information</b>  |  |
|  | 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<br>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<br>Global Root<br>CA | TWCA Global Root CA(Cross)  |  |
|                           | <b>Subject</b>  |  |
|                           | CN = TWCA Global Root CA<br>OU = Root CA<br>O = TAIWAN-CA<br>C = TW               |  |
|                           | <b>Certificate Related Information</b>  |  |
|                           | Serial Number: 40013353e4000000000000cca5d1b69                                    |  |
|                           | 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<br>8AD47F6D70A44FA80AF0F931125FFE3A76876FFAD219A4D40A13C038DC85E69E    |  |
| TWCA<br>Global Root<br>CA | <b>Issuer</b>   |  |
|                           | CN = TWCA Root Certification Authority<br>OU = Root CA<br>O = TAIWAN-CA<br>C = TW |  |
|                           | <b>Key Related Information</b>  |  |
|                           | 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<br>EVSSL<br>Certification<br>Authority | TWCA EVSSL Certification Authority   |  |
|   | Subject  |  |
|   | CN=TWCA EVSSL Certification Authority<br>O=TAIWAN-CA<br>C=TW   |  |
|   | Certificate Related Information  |  |
|   | Serial Number 400134da0a00000000000000782d7a0<br>Signature Algorithm: sha384RSA<br>Not Before: 2024-Sep-6 16:16:46<br>Not After: 2034-Sep-6 23:59:59<br>Thumbprint Algorithm: sha1<br>Thumbprint 92e92b121414b8c04248970fa62596aa138a81cc<br>Thumbprint Algorithm: sha2<br>Thumbprint<br>CAC9FD0CD35AA5C480CD03FDD6EDF0CA1A41FD02AC290EC83D83CEEDF8EC245C                          |  |
|   | Issuer   |  |
|   | CN=TWCA CYBER Root CA<br>OU=Root CA<br>O=TAIWAN-CA<br>C=TW   |  |
|   | Key Related Information  |  |
|   | Subject Public Key: RSA(4096 bits)<br>Authority Key Identifiers: 9d 85 61 14 7c c1 62 6f 97 68 e4 4f 37 40 e1 ad e0 0d 56 37<br>Subject Key Identifiers: 5b 3c ba 2c da 44 dd eb 5c 4e 3d ce ee 58 f8 2e 55 92 1b 7a<br>Basic Constraint: Subject Type=CA<br>Path Length Constraint=0<br>Key Usage: Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86) |  |
|   |  |  |



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