工商憑證管理中心

稽核報告

執行單位：安侯建業聯合會計師事務所

Independent Assurance Report

To the management of the Ministry of Economic Affairs：

Scope

We have been engaged, in a reasonable assurance engagement, to report on Ministry of Economic Affairs (MOEA) management's assertion that for its Certification Authority (CA) operations at Taipei and Taichung, Taiwan throughout the period April 1, 2023 through March 31, 2024 for its CAs as enumerated in Appendix, the MOEA has：

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
  - Ministry of Economic Affairs Certification Authority (MOEACA) Certification Practice Statement V2.4;
- Maintained effective controls to provide reasonable assurance that：
  - MOEACA Certification Practice Statement is consistent with GPKI Certificate Policy
  - MOEACA provide its services in accordance with its Certificate Policy and Certification Practice Statements
- Maintained effective controls to provide reasonable assurance that：
  - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
  - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles;

- subscriber information is properly authenticated for the registration activities performed by MOEACA

■ Maintained effective controls to provide reasonable assurance that：

- logical and physical access to CA systems and data is restricted to authorized individuals;
- the continuity of key and certificate management operations is maintained; and
- CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity

in accordance with the WebTrust Principles and Criteria for Certification Authorities V2.2.2.

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

MOEACA does not escrow its CA keys, and does not provide subscriber key generation services. Accordingly, our procedures did not extend to controls that would address those criteria.

Certification authority's responsibilities

MOEA's management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with WebTrust Principles and Criteria for Certification Authorities V2.2.2.

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, Engagements* 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.

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 MOEACA's key and certificate life cycle management business and its controls over key and certificate integrity, over the authenticity and confidentiality of subscriber and relying party information, over the continuity of key and certificate lifecycle management operations and over development, maintenance and operation of systems integrity;

(2) selectively testing transactions executed in accordance with disclosed key and certificate life cycle management business practices;

(3) testing and evaluating the operating effectiveness of the controls; and

(4) performing such other procedures as we considered necessary in the circumstances.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

The relative effectiveness and significance of specific controls at MOEA 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, MOEACA'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 April 1, 2023 to March 31, 2024, the MOEA management assertion, as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities V2.2.2.

This report does not include any representation as to the quality of MOEACA's

services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities V2.2.2, nor the suitability of any of MOEACA's services for any customer's intended purpose.

KPMG

Certified Public Accountants

Taipei, Taiwan, ROC

July 15, 2024

Appendix – List of MOEACA in Scope

<table>
<tr><td rowspan="6">MOEACA</td><td colspan="2">Subordinate CA Certificate</td></tr>
<tr><td>Subject</td><td>Issuer</td></tr>
<tr><td>OU=工商憑證管理中心
O=行政院
C=TW</td><td>O=Government Root Certification Authority
C=TW</td></tr>
<tr><td>Certificate Related Information</td><td>Key Related Information</td></tr>
<tr><td>Serial Number: 00 fd b3 f5 36 49 99 e6 4e 8c cb 36 62 12 90 e3 2b

Signature Algorithm: sha1RSA

Not Before: 2003-04-21 03:42:45 p.m.(UTC+8:00)

Not After: 2023-04-21 03:42:45 p.m.(UTC+8:00)

Thumbprint Algorithm: sha1
Thumbprint: 72 6f dc d7 01 e9 18 29 93 00 17 ec 2e 3d dc f1 3c 65 e7 0b

Thumbprint Algorithm: sha2
Thumbprint: 90 ff c5 15 0c e0 53 50 69 e7 e5 ef 96 1e 40 47 fb 08 61 a1 40 73 2c 8c ed c7 e8 d5 8e b5 9b d1</td><td>Subject Public Key: RSA(2048 bits)

Authority Key Identifiers: cc cc ef cc 29 60 a4 3b b1 92 b6 3c fa 32 62 8f ac 25 15 3b

Subject Key Identifiers: 82 ff de a1 8c 12 d4 eb 63 c7 61 a4 68 8b a1 a8 7c 8f 57 27

Basic Constraint: Subject Type=CA

Path Length Constraint=0

Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)</td></tr>
<tr><td>Additional Information</td><td>Remark</td></tr>
<tr><td>CRL Distribution Point: http://grca.nat.gov.tw/repository/CRL/CA.crl
Certificate Policy: 2.16.886.101.0.3.3</td><td>■ CA certificate of 1st Generation of MOEACA Certification Authority signed by GRCA</td></tr>
</table>

MOEACA – G2	Subordinate CA Certificate	
	Subject	Issuer
	OU=工商憑證管理中心 O=行政院 C=TW	O=Government Root Certification Authority C=TW
	Certificate Related Information	Key Related Information
	Serial Number: 00 87 29 cd 5c f9 0b fa b6 12 d2 6c 2f 9f 67 b6 dd Signature Algorithm: sha256RSA Not Before: 2013-01-31 11:29:20 a.m.(UTC+8:00) Not After: 2033-01-31 11:29:20 a.m.(UTC+8:00) Thumbprint Algorithm: sha1 Thumbprint: 83 e3 74 6c ea af ce b2 67 62 de 5a b5 7d d6 4b 03 a3 7f 58 Thumbprint Algorithm: sha2 Thumbprint: 0c f0 8b 01 e5 54 eb 76 31 d4 91 6e 9e 8c 53 98 af 99 42 42 a2 6c a3 88 63 86 22 a0 e5 9f f3 79	Subject Public Key: RSA(2048 bits) Authority Key Identifiers: d5 67 1d e0 9c 7a 2c 9c cb c5 98 e7 1d 07 26 2a 86 ec 74 cd Subject Key Identifiers: 99 44 7a 02 72 eb 6d 65 22 b3 02 57 8f d6 a1 dd 3a 02 0f 6c Basic Constraint: Subject Type=CA Path Length Constraint=0 Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)
	Additional Information	Remark
	CRL Distribution Point: http://grca.nat.gov.tw/repository/CRL2/CA.crl Certificate Policy: 2.16.886.101.0.3.3	■ CA certificate of 2nd Generation of MOEACA Certification Authority signed by GRCA-G2

MOEACA – G3	Subordinate CA Certificate	
	Subject	Issuer
	OU=工商憑證管理中心 O=行政院 C=TW	CN = Government Root Certification Authority - G3 O = 行政院 C = TW
	Certificate Related Information	Key Related Information
	Serial Number: 74 aa 46 e4 4a b8 88 d3 a8 b0 a0 c9 7b 6d b7 d1 Signature Algorithm: sha256RSA Not Before: 2022-06-07 11:20:00 a.m. Not After: 2042-06-07 11:59:59 p.m. Thumbprint Algorithm: sha1 Thumbprint: bb 2c c6 33 59 f0 36 a7 7a cb eb a7 80 a6 aa 0b 04 bd a1 d8	Subject Public Key: RSA(4096 bits) Authority Key Identifiers: 3a 90 8e e7 41 47 19 73 dc 9c bd a3 7e d8 3d 3e 83 09 1f 03 Subject Key Identifiers: 46 cc 59 f8 66 7c 73 6a 70 4b 8f f3 d6 18 13 e6 20 de 9c 68 Basic Constraint: Subject Type=CA Path Length Constraint=0 Key Usage: Certificate Signing, Off-line CRL Signing, CRL Signing (06)
	Additional Information	Remark
	CRL Distribution Point: http://grca.nat.gov.tw/repository/CRL3/CA.crl Certificate Policy: 2.16.886.101.0.3.3	■ CA certificate of 3rd Generation of MOEACA Certification Authority signed by GRCA-G3

經濟部
Ministry of Economic Affairs

工商憑證管理中心

管理聲明書

本管理中心於中華民國 112 年 4 月 1 日至 113 年 3 月 31 日期間之營運均依據憑證實務作業基準揭露之管控方式執行

中華民國 113 年 7 月 3 日

數位發展部委託安侯建業聯合會計師事務所（以下簡稱貴所）針對工商憑證管理中心執行獨立查核之工作。經濟部（以下簡稱本部）為工商憑證管理中心主管機關，提供下列工商憑證管理服務：憑證註冊、憑證更新、憑證金鑰更換、憑證簽發、憑證公布、憑證廢止、憑證狀態資訊維護。

本部工商憑證管理中心負責建立與維護工商憑證機構維運作業之有效控制，控制內容包括：

- 憑證機構營運管理控制
- 憑證機構金鑰與憑證管理相關控制
- 憑證申請者憑證生命週期管理相關控制
- 資訊技術及相關作業之控制
- 主管機關相關規範之遵循

任何內部控制的制度均有其先天上之限制，故上述內部控制的制度僅提供工商憑證管理中心維運作業有限之合理保證。除此之外，有可能

因為未來工商憑證管理中心系統設定或內部控制制度之變更，導致風險因素增加，而改變控制之有效性。

本部工商憑證管理中心已對工商憑證機構之維運進行內部評估，依評估結果，本部工商憑證管理中心所提供之憑證管理服務，業已：

- ■ 揭露其金鑰與憑證生命週期管理方式以及資訊保密措施，並依所揭露之內容進行憑證機構維運管理。
- ■ 實施有效維運控制以確保：
  - 憑證申請者之身分經工商憑證管理中心適當確認。
  - 所管理之金鑰與憑證其完整性得以建立及維護。
- ■ 實施有效維運控制以確保：
  - 憑證申請者與憑證信賴者之資訊為授權人員方可取得，且上述資訊未使用於業務揭露描述內容以外的用途。
  - 金鑰與憑證管理維運作業之持續性得以維護。
  - 憑證管理系統之開發、維護與操作經由適當授權與執行，以維護憑證管理系統之完整性。

工商憑證管理中心

經濟部

中華民國 113 年 7 月 3 日