Independent Assurance Report

To the management of the Ministry of Interior Affairs：

Scope

We have been engaged, in a reasonable assurance engagement, to report on Ministry of Interior Affairs (MOI) management's assertion that for its Certification Authority (CA) operations at Taipei and Taichung, Taiwan throughout the period April 1, 2018 through March 31, 2019 for its CAs as enumerated in Appendix, the MOI has：

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
  - Ministry of Interior Affairs Certification Authority (MOICA) Certification Practice Statement V1.9.1
- Maintained effective controls to provide reasonable assurance that：
  - MOICA Certification Practice Statement is consistent with GPKI Certificate Policy
  - MOICA 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 MOICA

■ 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 V2.1 and WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security V2.3 Principle IV.

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

MOICA 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

MOI'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 V2.1 and WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security V2.3 Principle IV.

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 MOICA'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.

Inherent limitations

Because of the nature and inherent limitations of controls, MOICA'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, 2018 to March 31, 2019, the MOI management assertion, as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities V2.1 and WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security V2.3 Principle IV.

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

MOICA's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities V2.1 and WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security V2.3 Principle IV, nor the suitability of any of MOICA's services for any customer's intended purpose.

KPMG

KPMG
Certified Public Accountants
Taipei, Taiwan, ROC
July 23, 2019

Appendix – List of MOICA in Scope

	Subordinate CA Certificate	
	Subject	Issuer
	OU=內政部憑證管理中心 O=行政院 C=TW	O=Government Root Certification Authority C= TW
	Certificate Related Information	Key Related Information
MOICA	Serial Number: 08 b5 d8 ab c8 0b dc ef 2c 7e 0f 39 0a 56 37 13 Signature Algorithm: sha1RSA Not Before: 2003-04-21 03:56:07 p.m.(UTC+8:00) Not After: 2023-04-21 03:56:07 p.m.(UTC+8:00) Thumbprint Algorithm: sha1 Thumbprint: 3e 21 d6 e3 9c 6f c0 8f 44 42 f3 7b 22 f3 c1 3a a1 a3 d9 9e Thumbprint Algorithm: sha2 Thumbprint: 45 11 14 50 fb 31 ef 51 37 e4 b7 cf f9 ee 2b ef 23 e8 bb fd 16 50 86 df bd 93 df 2f 32 9b 78 5e	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: b6 20 c8 cf be 51 8a a4 54 b9 78 d3 04 d1 0a b2 cc 7e 2f 46 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/CRL/CA.crl Certificate Policy: 2.16.886.101.0.3.3	■ CA certificate of 1st Generation of MOICA Certification Authority signed by GRCA

	Subordinate CA Certificate	
	Subject	Issuer
	OU=內政部憑證管理中心 O=行政院 C=TW	O=Government Root Certification Authority C=TW
	Certificate Related Information	Key Related Information
MOICA – G2	Serial Number: 51 c3 b5 c1 a9 a1 58 86 09 22 22 31 d6 1a c0 ad Signature Algorithm: sha256RSA Not Before: 2014-01-02 02:31:04 p.m.(UTC+8:00) Not After: 2034-01-02 02:31:04 p.m.(UTC+8:00) Thumbprint Algorithm: sha1 Thumbprint: 27 97 ef ff 19 ed d7 7e fd 2a fc 45 e2 32 53 66 14 f5 be f0 Thumbprint Algorithm: sha2 Thumbprint: c4 c4 62 de 46 3f 85 68 04 dc 89 83 38 d2 ce cb 55 fb a7 41 55 85 15 99 d8 fb 7d 70 21 8f d1 be	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: fa 9b 34 67 09 0a 98 22 f7 62 48 8b 82 26 a6 45 c5 c3 22 a4 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 MOICA Certification Authority signed by GRCA-G2