KPMG

工商憑證管理中心

稽核報告

安侯建業聯合會計師事務所（以下簡稱本所）業已審查經濟部（以下簡稱　貴部）於「電子化政府公開金鑰基礎建設外部稽核委外服務案（以下簡稱本案）」所提出之管理聲明書，該管理聲明書宣稱　貴部憑證管理中心於民國 105 年 7 月 1 日至民國 106 年 6 月 30 日期間之營運已依照美國會計師公會（AICPA）及加拿大會計師公會（CPA, Canada）所訂定之憑證機構認證稽核標準（Trust Service Principles and Criteria for CA V2.0）達成以下事項：

- 已於憑證實務作業基準揭露金鑰與憑證生命週期管理以及資訊隱私實務；並依照所揭露之內容提供服務。
- 維持有效之控制以提供下列事項之合理保證：
  - 憑證申請者之資訊經過適當的身份認證。
  - 已於金鑰與憑證之生命週期建立控制並保護所管理之金鑰與憑證之完整性。
- 維持有效之控制以提供下列事項之合理保證：
  - 限制憑證申請者及憑證信賴者之資訊僅由授權之對象接觸，並防止非憑證實務作業基準所揭露之使用。
  - 金鑰與憑證生命週期管理作業之持續性。
  - 憑證系統之發展、維護與操作經過適當之授權並適當地加以實施以維持憑證系統之完整性。

KPMG

貴部憑證管理中心為管理聲明書負責，本所職責係依據審查之結果對該管理聲明書表達意見。

本所執行之審查乃遵循美國會計師公會（AICPA）及加拿大會計師公會（CPA, Canada）所制定之憑證機構認證稽核標準（Trust Service Principles and Criteria for CA V2.0）執行，審查內容包括：

- 瞭解金鑰及憑證生命週期管理及資訊隱私實務
- 瞭解　貴部憑證管理中心對於以下項目所實施之控制：
  - 金鑰與憑證完整性
  - 憑證申請者與憑證信賴者之身份真實性與隱私
  - 金鑰與憑證生命週期管理作業之持續性
  - 憑證系統之發展、維護與操作
- 測試實際執行是否遵照所揭露的金鑰及憑證生命週期管理及資訊隱私實務
- 測試並評估控制執行之有效性
- 執行其他本所認為必要之審查

本所確信所執行之審查可做為本所表達合理意見之基礎。

依本所之意見，前述　貴部憑證管理中心所出具之管理聲明書，就民國105年7月1日至民國106年6月30日期間而言，為允當之陳述。

基於任何控制無法完全避免錯誤產生之限制，　貴部憑證管理中心之維運仍有可能發生錯誤或不當管控而未能發現。此外，依據本所審查發現所得之任何結論，於查核期間以外之時段亦可能受以下項目影響

而有風險：

- 對系統及控制所作之變更
- 資料處理需求之變更
- 隨時間演變所作之調整
- 政策或程序之遵循程度將改變該結論之有效性

貴部憑證管理中心之特定控制的有效性與重要性及其控制對於評估憑證申請者及憑證信賴者的風險管控之影響皆取決於彼此互通所需的控制與其它因素。本所未審查憑證申請者及憑證信賴者之控制的有效性。

本報告不包括任何有關　貴部憑證管理中心服務品質的表述，亦不包括　貴部憑證管理中心對於客戶所提供之任何服務適切性的表述，與貴部憑證管理中心委由外部單位進行之系統開發與測試活動。

安侯建業聯合會計師事務所

會計師

陳振乾

中華民國106年8月4日

Appendix

	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
MOEACA	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	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)
	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 MOEACA Certification Authority signed by GRCA

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	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