政府公開金鑰基礎建設憑證政策變更總說明

一、 背景說明

(一) 因應量子計算所帶來之安全風險，增訂支援後量子密碼學(Post-Quantum Cryptography, PQC)之規範，並微調現有RSA金鑰使用規定。

(二) 配合NIST FIPS 140系列標準之演進與發展，調整相關規範內容。

(三) 完善公開金鑰參數之管理與品質檢驗機制，以提升整體制度之安全性與一致性。

(四) 依RFC 3647建議架構，調整現行章節配置及內容編排。

(五) 修訂文件中多處文字說明，並配合調整部分內容敘述、文句編排、補充修飾內容及刪除不適用內容。

二、 修訂內容摘要

(一) 新增PQC相關規範說明並調整現行RSA使用規定。

(二) 修訂密碼模組規範標準。

(三) 修訂公開金鑰參數之產製及品質檢驗規範，明確RSA金鑰之適用範圍，並以金鑰品質檢驗取代原質數測試規定。

(四) 刪除與其他章節內容或性質重疊且未納入RFC 3647建議架構之章節。

(五) 修訂文件中多處文字說明，並調整文句編排、補充修飾內容及

刪除不適用內容。

三、修訂內容說明

(一) 新增PQC相關規範說明並調整現行RSA使用規定。

說明：因應量子計算對現行公開金鑰密碼技術(涵蓋簽章及加密機制)之威脅，新增PQC相關規範(包含金鑰長度、金鑰對使用期限及演算法物件識別碼)與名詞解釋，同時調整現行RSA金鑰使用規定，異動章節包含6.1.5、6.3.2.1、6.3.2.2、7.1.3及附錄1等章節。

(二) 修訂密碼模組規範標準。

說明：配合NIST對FIPS 140系列標準之發展及實務銜接需求，修訂密碼模組適用規範，同步納入符合FIPS 140-2或FIPS 140-3標準之密碼模組。另鑑於部分應用情境受平台或設備型態限制，爰增訂於該等情境下，得由憑證機構依其權責評估並確認具同等安全強度之密碼模組之相關規定，以兼顧實務運作需求及整體資訊安全，異動章節包含6.1.1與6.2.1。

(三) 修訂公開金鑰參數之產製及品質檢驗規範，明確RSA金鑰之適用範圍，並以金鑰品質檢驗取代原質數測試規定。

說明：配合國際標準及實務作業需求，修訂6.1.6節「公開金鑰

參數之產製與品質檢驗」相關規範，明確RSA金鑰之適用範圍，並以金鑰品質檢驗取代原質數測試規定，以提升規範一致性及適用性。

(四) 刪除與其他章節內容或性質重疊且未納入RFC 3647建議架構之章節。

說明：

1. 考量6.9節「密碼模組安全管控措施」內容為重述6.1節「金鑰對產製及安裝」與6.2節「私密金鑰保護及密碼模組安全控管措施」之規定，未新增實質規範，且此章節亦非RFC 3647建議架構之章節，故刪除此節，簡化文件架構。
2. 原1.4.2節、3.1.7節、3.2.7節、3.3.3節及5.7.5節亦有類似情況且非RFC 3647建議架構之章節，故同步刪除，簡化文件架構。

(五) 修訂文件中多處文字說明，並調整文句編排、補充修飾內容及刪除不適用內容。

說明：修訂文件中部份誤植文字、冗詞贅字、英譯用語、標點符號、文句寫法及遺漏內容，並調整文句編排、補充文句修飾說明及刪除不適用內容，此修訂不影響原意與實

務運作，異動章節包含1、1.1.3、1.2、1.4.2、1.5.1、1.5.4、2.2、3.1.2、3.2.1、3.2.5、4.2、4.2.1、4.7.3、5.3.1、5.4.8、5.7.4、6.1.5、7.3.1、7.3.2、8、8.1、8.2、8.5、9.5、9.10、9.10.1、9.10.2及附錄1等章節。