政府機關公開金鑰基礎建設技術規範
第 1.3 版變更總說明

一、 背景說明

團隊配合新專案合約要求進行檢視與修訂。

二、 修訂內容摘要

(一) 附錄新增有關後量子密碼(PQC)相關標準資訊，包含 FIPS 203、FIPS 204 及 FIPS 205。

(二) 修訂文件中多處文字說明，並調整文句編排與補充文句修飾說明。

三、 修訂內容說明

(一) 修訂 RFC 標準名稱。

說明：

(a) 修訂第 1 節 RFC 標準名稱，因 RFC 2527 已被 RFC 3647 所取代。

(b) 修訂第 4 節 RFC 標準名稱，因 RFC 3280 已被 RFC 5280 所取代。

(c) 修訂第 6 節 RFC 標準名稱，因 OCSP 有關的 RFC 標準已由 RFC 6960 取代 RFC 2560。

(二) 移除過時之演算法資訊。

說明：2.1.1 及 2.6 節 移除過時之 SHA-1 演算法資訊；2.4 節移除過時的 3-DES 與 RC-2 對稱金鑰加解密演算法資訊；第 7 節，更新 TLS 協定版本，現行國際規範要求至少為 TLS 1.2 或以上版本才安全。

(三) 依照國際規範修正應用端之金鑰長度

說明：2.3 節依照國際規範，修正 RA 跟 EE 的金鑰長度，改用「RSA 2048 bits（含）以上，或 NIST 制定的 PQC 標準演算法」。

(四) 修訂 API 呼叫規格資訊

說明：第 9 節新增新一代可用來建立加密安全性軟體，以進行加密密鑰管理、密碼編譯和數據安全性，以及密碼編譯和網路安全性之 CNG API 呼叫規格資訊。

(五) 修正標準名稱。

說明：第 10 節修訂稽核標準名稱為「WebTrust Principles and Criteria for Certification Authorities」及國際合規之密碼模組安全等級驗證標準名稱為「NIST FIPS PUB 140-2」。