

採購規範書

1. 目的/用途說明：執行「115 年中國信託銀行電子簽章試辦技術服務」，提供支援 NIST PQC 後量子簽章演算法之 USB Dongle 與客戶端 PQC 簽章代理程式，需採購支援 NIST PQC 後量子簽章演算法之材料模組 3 組。

2. 品名：支援 NIST PQC 後量子簽章演算法材料模組

3. 規格與功能需求

項目	品項/型號	規格說明	數量/單位
1	NIST PQC後量子 簽章演算法材料 模組	- 支援以下功能：1.支援對文件產生 PQC 簽章值。2.支援驗證文件完整性。 - 通過以下認證：1.模組之晶片符合共通準則(Common Criteria)ISO/IEC 15408 EAL4+ 或其他相同安全強度之認證。2.PQC 演算法(ML-DSA)通過 CAVP 認證。	3 組
2	維運保固	模組提供 1 年保固	1 式

4. 付款時間：廠商須於 115 年 10 月 10 日前交貨，經功能與證書驗收同意後付清費用。

5. 測試與證書佐證要求：

A.通過 1.支援對文件產生 PQC 簽章值。2.支援驗證文件完整性。功能測試。

B.繳交 1.模組之晶片符合共通準則(Common Criteria)ISO/IEC 15408 EAL4+ 或其他相同安全強度之認證。2.PQC 演算法(ML-DSA)通過 CAVP 認證。相關證書文件。

6. 保固：模組提供 1 年保固。

7. 教育訓練: 無