



購案名稱：PQC後量子加密安全連線導入技術服務

用途說明：

先進晶片產業前瞻技術發展計畫之晶片運算系統軟體，將保存團隊開發過程中的重要資料，其中包含高度敏感的技术機密。因此，開發環境及平台須具備高等級資訊安全防護能力，以確保資料不外洩。

晶片運算系統軟體運行於嵌入式系統平台，開發端與該軟體環境之間須建立安全且可信的通訊機制，此為整體系統安全之關鍵。本計畫將評估並導入符合零信任架構（Zero Trust Architecture）的安全通道技術，透過細緻化存取控制、強化身分驗證及連線授權管理，確保開發者、裝置與晶片運算系統軟體環境之間的連線安全。

此外，考量量子計算未來可能威脅現行密碼學機制，平台須支援後量子密碼學（Post-Quantum Cryptography, PQC），使通訊加密機制能抵抗量子計算攻擊，並相容於新一代密碼演算法（如 NIST 標準化之 ML-KEM、ML-DSA），以保障資料交換與長期傳輸的安全性。

服務規格及說明：

1. 後量子加密導入：協助部署採用 NIST 標準加密演算法（FIPS-203、FIPS-204、FIPS-205）之後量子安全 TLS 連線。
2. 架構規劃與整合：評估既有平台環境，規劃並完成整合，無需修改現有應用伺服器。
3. 相容性設定與測試：確保向下相容，使用端尚未升級至 TLS 1.3 或不支援後量子演算法時，仍能正常連線。
4. 演算法驗證依據：所採用演算法通過 NIST CAVP 認證（ML-KEM #A7024、ML-DSA #A8021、SLH-DSA #A8023）。
5. 服務範圍及期間：提供技術諮詢與問題排除。

交付項目：

1. PQC 後量子加密安全連線導入技術服務案（服務範圍以 3 個網站為上限）
2. 現場示範安裝服務
3. 安裝與使用說明手冊。

驗收方式：

1. 確認服務案及相關文件
2. 於工研院準備之嵌入式系統環境，透過服務案於集中式管理平台進行設定、使用者管理、存取政策設定，再於終端裝置上執行已安裝之軟體進行安全通訊連線，並使用集中式管理平台進行記錄檢查。功能均須符合規格。