Solution Brief

後量子準備
從加密敏捷性開始

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

為量子做好準備

隨著量子電腦即將打破傳統加密，您現在就需要採取措施保護您的資料。先竊取、後解密（HNDL）攻擊已經發生，網路攻擊者收集並儲存加密資料，目的是在未來使用量子電腦對其進行解密。

為後量子加密 (PQC) 做好準備，透過建立可信賴的環境來測試已準備好的 PQC 加密技術，並識別量子計算可能對您的基礎設施安全性造成的潛在影響，同時制定快速調整的應對計劃。

今年，NIST（美國國家標準與技術研究院）已經發布並標準化後量子加密 (PQC) 演算法，供各企業/組織採用以防範量子計算攻擊。 NIST 正式標準化這些演算法，全球的監管機構將根據 NIST 的 PQC 標準化流程發布法規要求。隨著法規的發布與合規需求，屆時各企業/組織將快速應對實施相關措施。

透過具有內建敏捷加密架構的 PQC 網路加密解決方案，來保護動態資料

為什麼現在就必須進行PQC？

將現有的加密方法轉換為後量子加密 (PQC) 需要大量時間，最佳策略是**現在就開始準備**。透過即早部署，您可以減少對企業內部和客戶的影響，並降低成本和風險，以確保在轉型過程中保持業務的持續運作。這也將使您的企業在 NIST 及其他產業的 PQC 法規發布後，能夠立即完全符合法規需求。量子攻擊已經在發生，尤其是 "先竊取，後解密 " (HNDL) 攻擊，立即採取行動是明智之舉，例如使用更長的對稱密鑰長度或帶外密鑰等過渡解決方案。這不僅能保護您的企業免受當前 HNDL 攻擊，還能讓您更好地準備實施後量子加密技術。

掃描QRcode 以獲取更多 HSE PQC 入門套件的資訊

使用 PQC 入門套件邁出第一步

搭配 Thales 高速加密器 (HSE) 的 PQC 入門套件是一款低成本的解決方案，協助企業建立測試環境，以加速在安全環境中測試量子抵禦措施的過程。在這個 PQC 實驗室中，您可以使用後量子密碼學和熵來模擬執行應用程式、傳輸資料等，以幫助您驗證架構。透過今天的準備，您將制定一個行動計劃，確保在演算法最終整合到韌體後，業務運作能順利進行。

透過以下方式輕鬆設定量子安全測試環境：

- ✓ **預先實施 NIST 後量子演算法**
- ✓ **帶外密鑰管理，NIST認可的KDF方法**
- ✓ **可選功能的量子密鑰分發 (QKD)，符合 ETSI eQKD v14.01 標準**
- ✓ **可選QRNG（量子隨機數生成器）或外部熵源（BYOE—自帶加密方案）**

HSE PQC 入門套件包含項目

此入門套件配備功能齊全的 HSE ，可將其直接投入生產環境中，為現有網路提供額外的安全性和效能提升。

- **從 Thales HSE 產品組合中，選擇 3 款 HSE 網路加密設備**
  - **CN4010/CN4020:** 高達 1 Gbps 的網路加密器，經認證、高效能、小尺寸，非常適合 CNI、SCADA、語音/視訊等遠端位置
  - **CN6010:** 1 Gbps 網路加密器，機架安裝式，具備完全冗餘的堅固設計，非常適合專用網路和資料中心
  - **CN6140:** 高達 4x10 Gbps 網路加密器，具備 4 個獨立加密通道以實現擴展性，支援高可擴展性和多鏈路網路
- **CM7 Network Manager – 加密管理平台（可從客戶入口網站下載）**
- **推薦新增項目**
  - 電源線（CN6000系列型號）
  - 收發器（特別適用於 CN6000 和 CN4020 裝置）
  - 維護和支援
  - 遠端安裝與配置