



名家訪談

量子威脅如國安等級防禦戰

TWCA 積極佈建生態系聯防

隨著量子計算技術突飛猛進，全球金融產業即將面對前所未有的資安挑戰；量子電腦的發展不僅是未來式，更是亟需正視的現在進行式。為深入探討此議題，本刊特專訪臺灣網路認證公司（TWCA）總經理郭昭宏，請他剖析量子計算技術的影響，及金融機構應如何制定戰略藍圖，並強化數位韌性。

郭昭宏指出，量子電腦現已是金融資安的重大威脅，且金融界預估，「穩定且夠強大」的量子電腦將於 2030 年至 2035 年之間問世，即使當下加密數據看似安全，但攻擊者仍可能利用「先竊取、後解密」的手段，先蓄積關鍵交易資料，待日後技術突破後，再進行解密。

金管會已公佈遷移指引

此手段直接撼動了奠基於 RSA（Rivest-Shamir-Adleman）、ECC（Elliptic Curve Cryptography，橢圓曲線密碼學）等非對稱演算法的金融業傳統信

任鏈。郭昭宏直言，一旦現行加密架構失效，不僅將導致使用者帳戶資料外洩，更將面臨數位簽章「不可否認性」（Non-repudiation）崩潰的嚴峻危機，對金融體系造成劇烈衝擊。

為防範危機於未然，金管會於 6 月 18 日公佈金融業後量子遷移指引。郭昭宏強調，唯有建立「生態系聯防」，方可落實遷移指引，夥同 L1 的核心交換樞紐（如財金公司），到 L2 與之對接的金融機構，及更深一層的 L3 自主業務系統，與 L4 的第三方供應商，共築 5 大技術防護牆。

設定 4 個明確遷移階段

「在 2026 年，預計將完成 TWCA 端通訊及加密準備，並將雜湊函數升級至 SHA 2，希望協助客戶端在 2027 年完成升級。」郭昭宏透露，TWCA 將密切關注國際標準（如 Adobe AATL Root 及 CA/Browser）與主管機關（如銀行公會）的動態，再決定電子文件簽署類服務如何改變，「FXML 預

金融機構 後量子因應措施五大面向

關鍵面向	過渡策略（Now～至 2030）	遷移策略（2030~2035）	關鍵應用情境 / 註記
1. 通訊安全	TLS 1.3 • 全面汰換 TLS 1.2 以下版本，禁用過時的加密套件。 • 結合傳統 +PQC 的金鑰交換演算法，例如：X25519MLKEM768		網站連線、FTPS、VPN。
2. 加密保護	AES-256 對稱加密提升至 256-bit（對抗 Grover 演算法）。		資料庫加密、檔案存儲保護。
3. 數位簽章	SHA-2 以上 強化雜湊函數長度，捨棄 SHA-1。	PQC 簽章演算法 導入 ML-DSA（Dilithium）或 SLH-DSA（Sphincs+）。	• 數位身分識別 • 交易 • 電子合約
4. 憑證體系	RSA-2048 以上 / ECC • 調高傳統金鑰長度以延長存續期。 • 縮短憑證效期（如：TLS）。	PQC 數位憑證 建立支援 PQC 演算法的 PKI 體系。	• 國際標準、瀏覽器及平台。 • 股票下單憑證、FXML 轉帳、TLS 網站憑證
5. 載具 & 硬體	詢問供應商 PQC 方案		網路設備、IC 卡、HSM



臺灣網路認證股份有限公司總經理 郭昭宏

計於 2028 年提供新一代安控系統，而證券 EC+ 憑證是否升級，因涉及 PQC (Post-Quantum Cryptography，後量子密碼學) 金鑰尺寸更動，預計於 2031 年，待通訊及作業系統等基礎建設提升後啟動。」

在時間維度上，金管會設定了 4 個明確的遷移階段，依次為「準備與規劃階段」(2025 年至 2026 年)、「試辦與基礎升級階段」(2027 年至 2029 年)、「優先遷移階段」(2029 年至 2032 年)與「全面遷移與收斂階段」(2032 年至 2035 年)。郭昭宏表示，TWCA 已積極規劃各項服務的遷移時程。

「金融機構應依照金管會設定的 4 個階段，循序精準佈局。」郭昭宏解釋，在「準備與規劃階段」，應完成密碼資產盤點與權責建立，進入「試辦與基礎升級階段」後，應進行核心技術的 PoC (Proof of Concept) 驗證，到了「優先遷移階段」，應鎖定高風險、高敏感、長效期系統，並優先導入，而跨入「全面遷移與收斂階段」，則應完成整體體系的合規與固守。

有鑑於量子電腦技術尚不穩定且成本高昂，諸多硬體安全模組 (HSM) 與 IC 卡安全規定認證仍在進行，郭昭宏建議，目前金融機構宜採「過渡」(兼用傳統演算法和後量子演算法)與「遷移」(直接導入後量子演算法)並行策略，不必直接採取「對抗」(以量子電腦對抗量子威脅)策略。

協助金融機構因應危機

除了憑證體系，TWCA 亦積極關注 FIDO 無密碼驗證與區塊鏈技術的演進。郭昭宏認為，TWCA 將儘早引進符合後量子標準的驗證規格，確保未來的生物識別與金鑰交換機制，可無縫對接量子演算法，「區塊鏈底層高度依賴 ECC 演算法，未來勢必飽受

量子技術威脅，加上其去中心化架構的特質，現並無單一權責機構推動其升級，更應密切注意。」

TWCA 亦將依循金管會的指引與所規範的時程，針對 TWID 身分驗證中心的各項服務，協助各金融機構採取相應的因應措施。目前，TWCA 所提供的服務，可分為基礎建設 (如 TWCA Server 對外通訊)、CA 類 (TLS 網站憑證、銀行 FXML 憑證及證券 EC+ 憑證)、TWID 服務 (如 MID 身分識別、FIDO 驗證等)、電子文件簽署類 (如電子保單、電子文件簽署) 等。

臺灣金融產業如何因應量子技術威脅？郭昭宏提出 3 點建議，分別為治理先行、務實合規、生態互助。治理先行，指各金融機構應儘速建立後量子治理架構，將密碼資產管理列入年度重大風險監控事項中，並調動各部門資源、人因應之，不可單純視量子技術威脅為 IT 部門的工作。

金融業業者最忠實夥伴

現階段金融機構不必因國際技術尚未全面到位而過度焦慮，當下應優先完成基礎環境升級 (如提升至 TLS 1.3、AES-256、SHA-2)，當可為企業爭取最關鍵的 5 年「從容期」。生態互助，則指 TWCA 將持續扮演主管機關與金融業業者之間的橋樑，並將動態對接最新的國際規範與臺灣法規。

「TWCA 是國家級的 CA (Certificate Authority，數位憑證認證機構)，也是臺灣金融業業者最忠實的夥伴。」郭昭宏充滿信心地說，TWCA 將持續推動憑證技術標準化與硬體兼容測試，確保在相關法令落地之刻，臺灣的金融基礎設施已經準備就緒，完成從傳統時代到量子時代的華麗轉身。