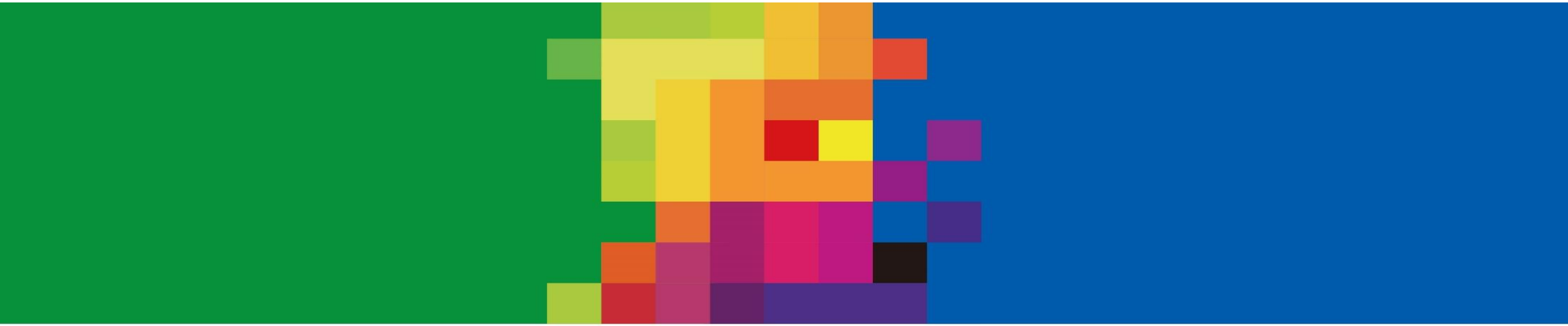
證交所券輔部教育訓練

PQC 金融實務分享

TWCA 協理 連子清



TWCA 臺灣網路認證

TWID 身分識別中心



量子電腦對金融業的威脅與挑戰

Copyright of TWCA

量子位元 (Qubit)

量子位元 (qubit) 是量子電腦的核心。qubit 會被製作在一個「量子處理晶片 (Quantum Processor Chip)」上。

項目	傳統晶片 (CPU/GPU)	量子晶片
運算單位	bit（0 或 1）	qubit（0 和 1 疊加）
工作環境	常溫可用	需要極低溫、真空、雷射或特殊光學設備
製程	矽晶片製程	多種技術：超導、離子阱、光子、拓撲量子等
穩定性	非常成熟	qubit 脆弱、容易受噪音干擾，需要糾錯

- **超導量子晶片**：看起來像一片金色的小板子，上面有很多微小電路，利用超導材料（例如鋁、鈮）製作。必須放在接近「絕對零度」的冰箱（稀釋冷凍機）裡才能運作。
- **離子阱晶片**：晶片上有「電極結構」，用來抓住單顆離子，並用雷射操控它們。
- **光子量子晶片**：晶片裡有微小的光學波導，用來控制光子走向，進行量子運算。

Copyright of TWCA

量子的三大特性

主要用來描述微觀世界（如電子、光子、原子等）

量子疊加 (Superposition)　同時是 0 又是 1



- 與傳統的物理狀態在某一時間只有一個特定狀態不同，量子狀態可以在同一時間具有不同的狀態。

量子糾纏 (Entanglement)　不管多遠都牽連在一起



- 兩個或多個粒子的量子狀態相互連接的量子力學現象，使得一個粒子的狀態立即與另一個粒子的狀態相連，無論它們之間的距離有多遠。

量子測量 (Measurement) 測量就會改變狀態



- 一但進行偵測，量子疊加就會瞬間塌縮，瞬間被迫選邊站變成確定的 0 或 1。

Copyright of TWCA

量子電腦的演算法及對加密的威脅

因為傳統演算法無法發揮量子的特性，科學家才開發了專屬的量子演算法。

對稱加密：Grover's Algorithm（葛羅佛演算法）

- 葛羅佛演算法可用於加速暴力破解：
  - 原本需嘗試 2^n 才能找到密鑰；
  - 現在只需約 $2^{\frac{n}{2}}$ 次。
- 影響：
  - 對稱加密安全強度減半。
  - 如：AES 256 bits 面對量子電腦的強度只剩下 128 bits。

非對稱加密：Shor's Algorithm（肖爾演算法）

- 肖爾演算法能在多項式時間內解決：
  - 整數因式分解問題（RSA）
  - 離散對數問題（DSA, DH）
  - 橢圓曲線離散對數問題（ECC）
- 這些問題在傳統電腦上需指數時間破解，但量子電腦將徹底打破這些「難解性」。
- 影響：
  - 傳統電腦破解 2048-bit RSA 需要數百年；量子電腦（一旦夠大）可能在幾小時內破解。

量子電腦 對 非對稱式演算法 的威脅 > 對稱式演算法

Copyright of TWCA

量子 和 後量子 的差別

比較維度	量子電腦 (Quantum Computing)	後量子密碼學 (Post-Quantum Cryptography, PQC)	關鍵關聯 / 說明
本質與定義	利用量子力學原理進行極高速運算的硬體技術，能執行蕭爾演算法等，從根本上瓦解現行密碼體系。	在傳統電腦上執行的全新數學密碼演算法，基於量子電腦也無法輕易破解的數學難題。	後量子密碼（PQC）是為了抵禦量子電腦攻擊而生的防禦盾牌。
使用技術與核心原理	• 超導電路、離子阱、中性原子、光量子等硬體。 • 依賴量子位元（Qubits）、量子糾錯（QEC）來對抗雜訊。	• 依賴格基密碼（Lattice-based 如Kyber/Dilithium）、多變數密碼等。 • 透過軟體及現有硬體架構進行升級替換。	技術層級完全不同：一個是物理的突破，另一個是傳統電腦上位資安演算法演進。
目前發展階段	• 從 NISQ 時代跨入容錯量子計算（Fault-Tolerant）的工程化關鍵期。 • IBM 規劃在2029 推出擁有大規模邏輯量子位元的容錯量子電腦	• 海選(R1:2016/12-2018; R2:2019/1~2020;R3:2020/7~2022,公佈結困,R4 持續進行) • 2024/8 NIST公佈FIPS 203,204,205	量子發展逼迫 PQC 必須加速落地，形成「攻擊」與「防禦」的賽跑。

Copyright of TWCA

先保存 後破解　夠強大且穩定的量子電腦預計在 2030 年問市。

威脅類型	說明
破解公鑰演算法	使用 **Shor's Algorithm** 破解 RSA、DH、ECC 等，取得私鑰與機密資訊。
偽造數位簽章	產生合法但偽造的電子簽章，導致文件、交易、程式碼簽章遭偽冒。
延後破解風險	「**先保存，後破解**」
以憑證為例	假設憑證效期為 1 年，Y= 1 年。 假設夠強大的量子電腦在2030年底推出，Z= 5 年。

若 X + Y 須 > Z，就需擔心

Y= 資料保存時間
X = 遷移至後量子的時間
Z= 量子電腦出現時間



Copyright of TWCA

後量子密碼遷移大事記

- 2022年9月
  - 美國國安局（NSA）發布 **CNSA 2.0**（商用國家安全演算法套件第二版）
- 2024年8月
  - NIST 正式公佈三項 PQC 提案 (FIPS 203:ML-KEM 適用加密, FIPS 204:ML-DSA 適用簽章, FIPS 205:SLH-DSA 適用簽章)
- **2025 年 4月**
  - **數發部發佈後量子遷移指引，要求供應商提供後量子準備QA**
- **2026 年6月**
  - **金管會發佈金融業後量子遷移指引。**

- **2027年1月1日**
  - 所有國家安全系統的新採購須支援 CNSA 2.0 (後量子)。
- **2030年12月31日**
  - 全面棄用 (Deprecation) 不符合 CNSA 2.0 的演算法（如:RSA 2048)
  - 舊演算法 (如: RSA) 尚可使用，但已不被建議用於新的系統或應用場景。
- **2032年**
  - **於2032年後強制新上線系統須使用符合CNSA 2.0的演算法**
- **2035年**
  - 全面禁用 (Disabling) 舊有演算法 (如:RSA, ECC等)，現有系統必須完成轉移或淘汰。

Copyright of TWCA

CNSA 2.0 演算法要求

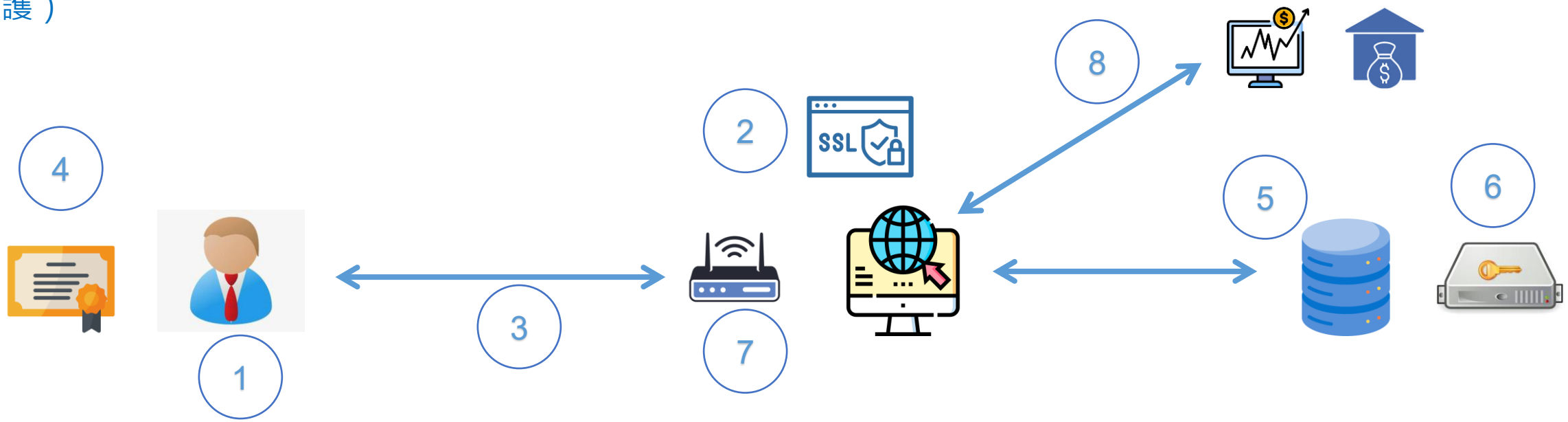
General Purpose Algorithms

Algorithm	Function	Specification	Parameters	
Advanced Encryption Standard (AES)	Symmetric block cipher for information protection	FIPS PUB 197	Use 256-bit keys for all classification levels.	對稱加密
ML-KEM (previously CRYSTALS-Kyber)	Asymmetric algorithm for key establishment	FIPS PUB 203	ML-KEM-1024 for all classification levels.	金鑰交換
ML-DSA (previously CRYSTALS-Dilithium)	Asymmetric algorithm for digital signatures in any use case, including signing firmware and software	FIPS PUB 204	ML-DSA-87 for all classification levels.	數位簽章
Secure Hash Algorithm (SHA)	Algorithm for computing a condensed representation of information	FIPS PUB 180-4	Use SHA-384 or SHA-512 for all classification levels.	雜湊函數

Copyright of TWCA

證券商可能受影響的場景

- 如：下單系統、基金交易/電商平台 HTTPS 通訊、線上簽署電子合約、客戶身分驗證及長效期投資資料防護)



1. 會員帳號密碼
2. 網站主機的 TLS 憑證
3. 客戶和主機的通訊加密 (https, ftps等)
4. 客戶下單憑證
5. 長效期資料防護 (數位簽章 + 金鑰加密)
6. 通訊設備 (如: VPN)
7. 金鑰儲存設備 (如: HSM)
8. 與交易所的交易或資料傳輸

Copyright of TWCA

因應量子威脅
之核心策略與技術演進

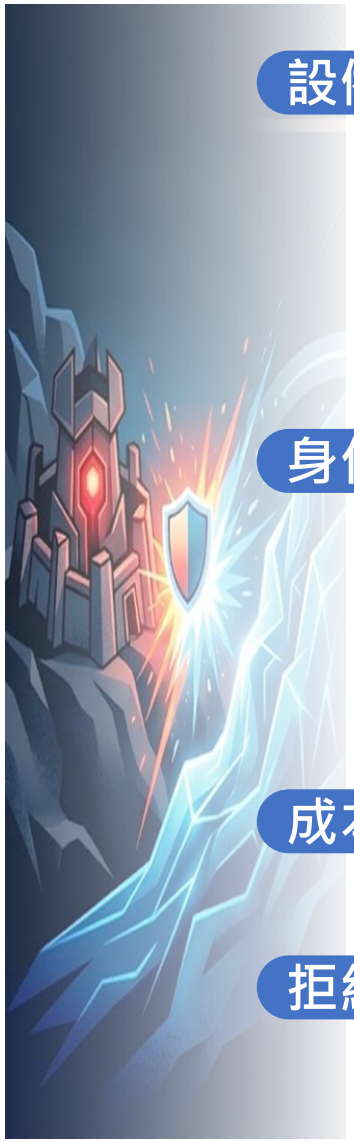


Copyright of TWCA



Copyright of TWCA

用量子電腦對抗量子威脅？



設備不容易實現

- 要實現理想的量子環境不容易，如：單光子源、弱雷射脈衝、絕對零度。
- 旁路攻擊 (Side-channel Attacks)，QKD 設備的某些物理特性（如:電磁輻射、功耗或時間、容易成為目標）。
- 光子在光纖中傳輸會衰減，故需增加信任中繼節點或衛星 QKD，但這也會增加信任問題。

身份驗證仰賴傳統機制

- QKD 本身只負責金鑰的分發，不提供通信雙方的身份驗證。如果攻擊者能冒充其中一方進行中間人攻擊 (Man-in-the-Middle Attack)，即使金鑰分發過程本身是安全的，通信仍會被竊聽。因此，QKD 系統需要依賴傳統的身份驗證機制（如公鑰基礎設施或預共享金鑰），這可能會重新引入經典密碼學的漏洞。

成本太高

- QKD 設備成本太高

拒絕服務攻擊 (DoS) 不易克服

- 量子通道具絕對的敏感性和物理特性，檢測即中斷，不易克服 DoS。

量子電腦仍有限制

Copyright of TWCA

演進的作法



因為後量子還需許多配套才能完成 **遷移**，國際 CA/Browser Forum 也在討論各種 **演進** 的作法。

現有演算法

演進 (Transition)

- 複合憑證 (Composite Certificate)
- 雙軌憑證 (Hybrid Certificate)
- 巢狀加密 (Nested/Wrapper)
  - 電子合約：外層對稱式加密+內層非對稱式簽章
  - TLS 1.3：外層 PQC 對稱式加密保護 非對稱式金鑰的交換
- 版本協商 (Negotiation)

遷移 (Migration)

後量子 (PQC)

- ✓ 目前 X.509 規格已公佈對 PQC 演算法的支援
- ☐ 瀏覽器支援作法 (通訊金鑰加密已支援, TLS 憑證討論中)
- ☐ 硬體支援 (如:IC卡,HSM均在認證中)

摘要自 CA/B Forum 2026/3

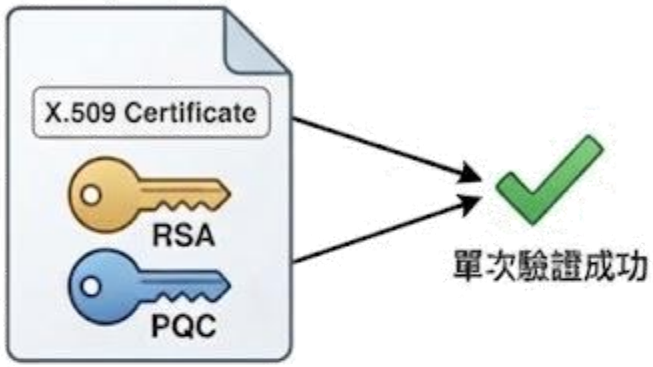


Copyright of TWCA

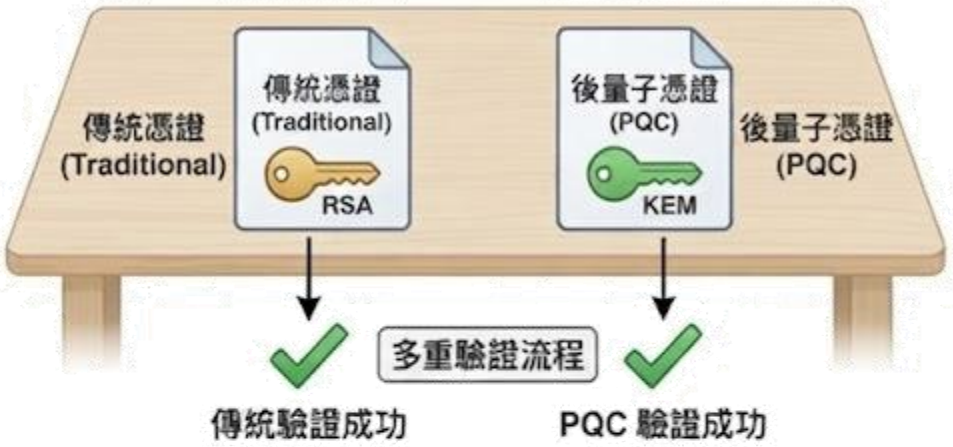
常見的演進作法

一張憑證同時具備傳統及 PQC 金鑰及簽章

1. 複合憑證 (Composite)



2. 雙軌憑證 (Hybrid/Dual)



兩張憑證分別具備傳統及 PQC 金鑰及簽章

非對稱式簽章+外層對稱式加密

3. 巢狀加密 (Nested/Wrapper)



4. 憑證自動化 (Certificate Automation)



縮短憑證效期及憑證自動化

Copyright of TWCA

不同策略重點及代表技術

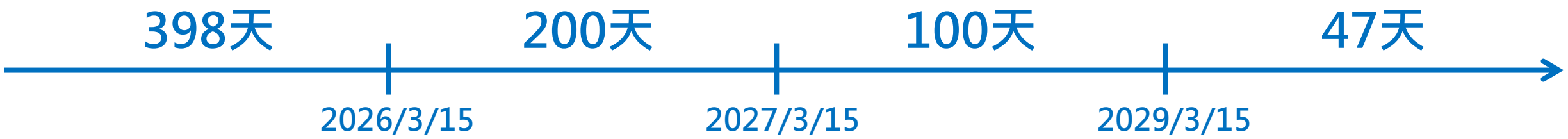
類型	策略重點	代表技術/作法	核心目的
1. 對抗	量子物理防禦	QKD (量子密鑰分發)	以物理定律確保傳輸安全
2. 演進	**技術轉型**	Composite / Hybrid / Nested	演算法平滑接軌、相容性
	治理強化	憑證自動化 / 效期縮短	縮短效期降低金鑰被破解的風險，並同時提升密碼敏捷性的韌性
3. 遷移	全新標準	Native PQC (ML-KEM / ML-DSA)	徹底移除弱加密，效能最佳化

同時採用 "**演進**" 和 "**遷移**" 是業界目前最常採用策略。

Copyright of TWCA

TLS 憑證效期縮短期程

- 2025/4/12 國際規範通過，TLS 憑證效期將逐年縮短
  - 基於安全因素 **(金鑰破解風險、憑證廢止空窗期、PQC 密碼敏捷性議題)**
- 這項規範**只針對 TLS 憑證**，**不影響**下單憑證及證期共用憑證。

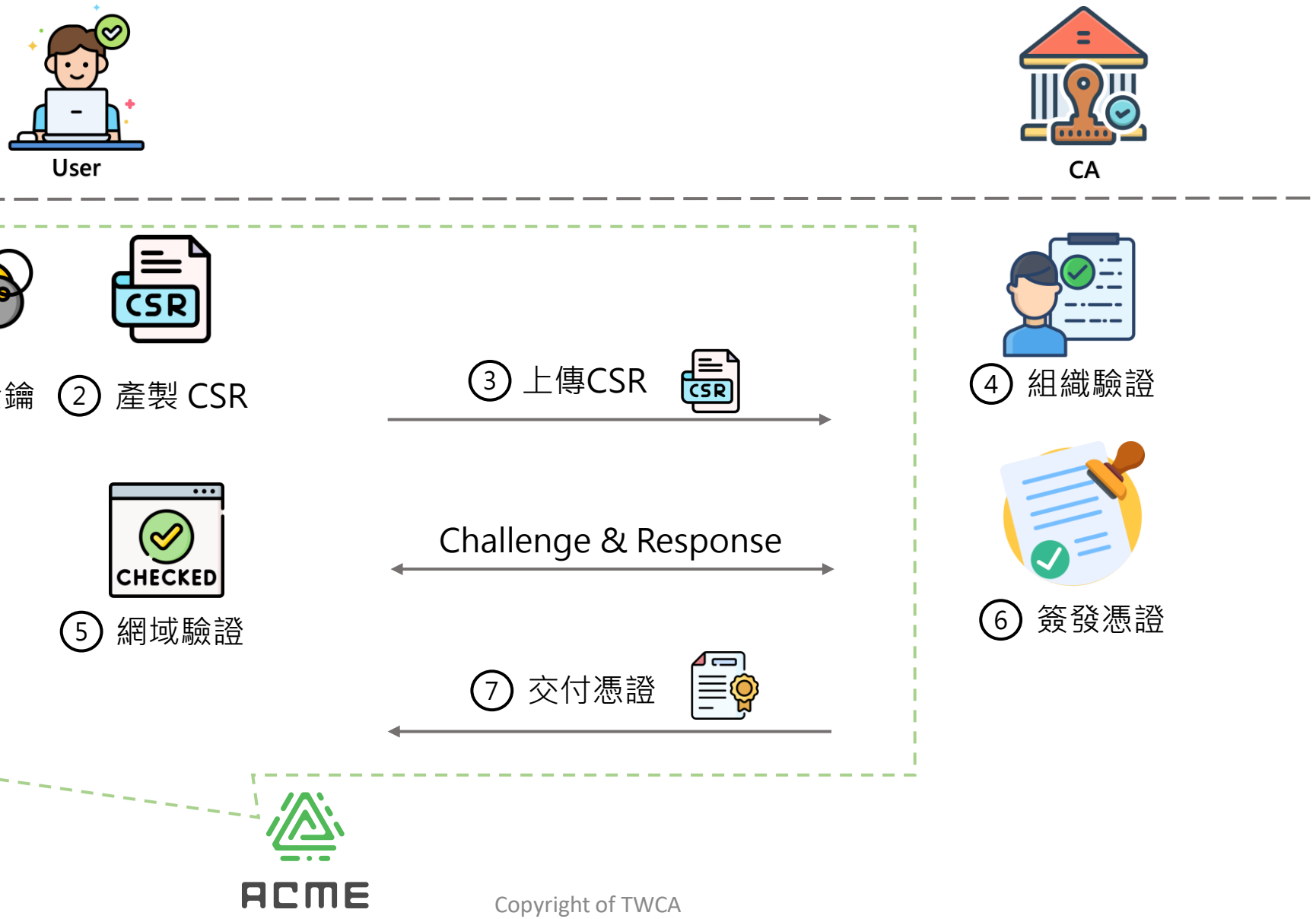


- **目前 TLS 憑證效期為 200 天，未來將逐年縮短至 47 天**

→ 盡早導入 **憑證自動化** 解決方案，採用支援自動化機制之 CA

Copyright of TWCA

ACME 可以做到哪些自動化？



Copyright of TWCA

憑證自動化解決方案

憑證申請流程	未導入自動化前	解決方案
產製金鑰	使用工具產生 (例如 OpenSSL)	**自動化，內含在 ACME 協定中**
產製 CSR	使用工具產生 (例如 OpenSSL)	**自動化，內含在 ACME 協定中**
上傳 CSR	將 CSR 貼入 CA 提供之窗口 (或使用選擇檔案方式上傳)	**自動化，內含在 ACME 協定中**
組織驗證	由 CA 自行完成，自動為主，必要時人工	由 CA 提供
網域驗證	HTTP、DNS、EMAIL、甚至電話驗證，透過人工方式放置 token	**自動化，內含在 ACME 協定中** **(僅支援自動化驗證方式)**
簽發憑證	由 CA 自行完成	由 CA 提供
交付憑證	CA 核發憑證後將憑證檔案寄給用戶	**自動化，內含在 ACME 協定中**

Copyright of TWCA

自動化解決方案比較

方案	說明	優點	缺點
Agent Base (TWCA)	• 地端主機安裝 Agent • 主要透過腳本方式支援基本的憑證佈署功能 • **適合環境單純的中小企業**	• **輕量化，導入速度最快** • 開源 Agent 取得容易，資源豐富 • 成本最低	• **僅提供佈署腳本執行功能，腳本內容需自行撰寫** • 需要具備佈署腳本撰寫能力 • 沒有多元的管理功能
CLM 平台	• 知名資安廠商： KeyFactor、Venafi (CyberArk)(PaloAlto)、appviewX、Entrust、HashiCorp(IBM)... 或各大 CA 自行開發 • 有 Agent Base (每台憑證主機安裝 agent) 也有集中式管理 (地端安裝專用主機) • 提供管理介面供管理人員對所有憑證主機進行操作 • **適合環境複雜、憑證張數多的大型企業**	• **針對特殊網路設備的佈署支援較高，或是內建佈署腳本** • 提供管理網站 • 提供其他額外管理服務 • 提供顧問諮詢，協助佈署導入	• **費用較為高昂，動輒數百萬** • 管理介面複雜
自行開發	• 透過 Agent 完成自動化申請憑證 • 自動化佈署透過自行開發或整合 (例如透過 Ansible) • **適合自主掌握程度或具有開發能力的企業**	• **自主性最高** • 可依企業內部實際情況做功能調整	• **需要具備開發整合能力** • 額外整合成本

Copyright of TWCA



密碼資產盤點與遷移優先順序矩陣

Copyright of TWCA

密碼資產盤點的原則及作法



快篩

- 全面及簡單



問診

- 細部盤點
- 遷移優先順序評估



關鍵資產檢查

- CBOM（外部工具或廠商提供）
- 供應商協助

Copyright of TWCA

金管會後量子遷移時程規劃

資料出處:金管會後量子遷移白皮書 (2026/6/18)

階段	建議時程	重點工作
準備與規劃	2025–2026	● 建立治理架構與盤點方法。 ● 盤點對外TLS端點與關鍵PKI/CLM/KMS/HSM。 ● 建立CBOM黃金資料來源。 ● 啟動供應鏈準備度治理與採購文件更新。 ● 建立測試案例與版本基準雛形。 ● 逐步提升既有演算法至安全性較高的演算法(如3DES升級為AES 256、SHA 1升級為SHA 2) 。
試辦與基礎升級	2027–2029	● 選定可控情境進行PoC / 試辦。 ● 測試混合模式（Hybrid Mode），評估對交易延遲與硬體效能的衝擊。 ● 提升TLS 1.3覆蓋率並清理反密碼模式。 ● 導入或強化憑證自動化與金鑰治理。 ● 建立切換與回退演練。 ● 開始建立跨機構共同測試窗口。
優先遷移（高風險/高關鍵）	2029–2032	● 依量子風險評分與外部互通窗口，優先推動對外通路、跨機構介接、關鍵驗章/簽章與高敏感長效期資料之遷移。 ● 導入PQC或混合模式並完成端到端測試；同步處置「卡關元件」汰換。
全面遷移與收斂	2032–2035	● 擴大至剩餘中低風險情境與長尾系統。 ● 完成跨體系PKI與信任鏈一致化。 ● 針對需LTV之既有存證/歸檔資料完成分期處置。 ● 建立常態化的演算法迭代與例行升級流程。

Copyright of TWCA

密碼資產盤點的角色類型

資料來源: F-ISAC PQC 遷移實務作業參考手冊 (115/9/1)

L1 HUB

- 財金公司 (31項)
- 聯卡中心 (13項)
- 聯徵中心 (7項)
- **集保結算所 (11項)**
- **證交所 (12項)**
- **期交所 (8項)**
- **櫃買中心 (14項)**
- 保發中心 (7項)
- 產險公會 (4項)
- 壽險公會 (6項)
- 地震基金 (1項)

合計11家,115項業務

L2 對接單位延伸

L3 單位自主業務

L4 供應商

密碼資產指有用到演算法的服務或資料，

由於金融領域的交易經常有上下游或 HUB，故我們將角色區分為三種類型 (L1, L2, L3)，另外 L4 供應商則是解決方案的提供者，未來在進行遷移時也需一併考量。

Copyright of TWCA

證期業者 L1 受影響的業務

證交所

1. 證券市場交易平台，包含股票交易、指數計算、行情傳輸及盤後資訊等功能
2. 證券商因交易傳輸系統發生重大不可抗力事故，致競價設備故障時，提供證券商借用市場備用之競價設備
3. 提供承銷案件（IPO、增資等）線上投標、開標配售、帳務處理與保證金扣退作業
4. 提供證券商申報服務，主管機關及周邊單位監理作業
5. 提供證券商「借券、結算、鉅額交易、ETF」等相關申報作業以及交易系統與周邊系統檔案傳輸
6. 提供上市（櫃）公司自行輸入之各項財務、業務及重大資訊。內容包括上市（櫃）公司之常用報表、基本資料、彙總報表、股東會及股利、公司治理、財務報表、重大訊息與公告、營運概況、投資專區、認購(售)權證、債券及資產證券化等相關資訊，並供大眾查詢
7. 提供證券商申請主機共置及其相關加值服務
8. 提供證券商申請競價設備、線路與測試申請等服務
9. 處理國內外資訊商、證券商與期貨商的資訊費、連線處理費等收費業務
10. 提供資訊公司申報用戶作業
11. 證券市場結算交割款及擔保金等的出入金資訊處理，並接收央行及銀行入金訊息且處理出金及放券作業
12. 證券交易相關機構透過平台互傳業務資訊，增強電子商務的商機、增加有效的管理資訊、減低交割風險、強化客戶支援與服務、提昇整體競爭力等多樣化效益。

合計 12 項業務

產險公會

1. 期貨交易服務
2. 提供店頭衍生性商品集中結算服務
3. 提供期貨商輸單服務
4. 提供CCP網路試算功能服務
5. 提供期貨商進行申報作業
6. 提供交易人線上查詢個人資料
7. 提供線路管理系統的線路申請與查詢
8. 提供結算會員虛擬帳號入金功能

合計 8 項業務

保發中心

1. 興櫃股票、開放式基金及黃金現貨買賣業務(含改帳)
2. 債券(公債、公司債、國際債、外國債)買賣業務
3. 衍生性金融商品交易業務
4. 衍生性金融商品交易申報業務
5. 上櫃股票買賣業務
6. 證券商財務申報業務
7. 上櫃公司及興櫃公司之財務及業務申報業務
8. 創櫃公司財務及業務申報業務
9. 上市公司、上櫃公司、興櫃公司及創櫃公司之經營實績申報業務
10. 交易資訊申請使用業務
11. 證券商經營股權性質群眾募資申報業務
12. 債券款券交割業務
13. 虛擬資產服務商申報業務
14. ETF鉅額詢價業務

合計 14 項業務

Copyright of TWCA

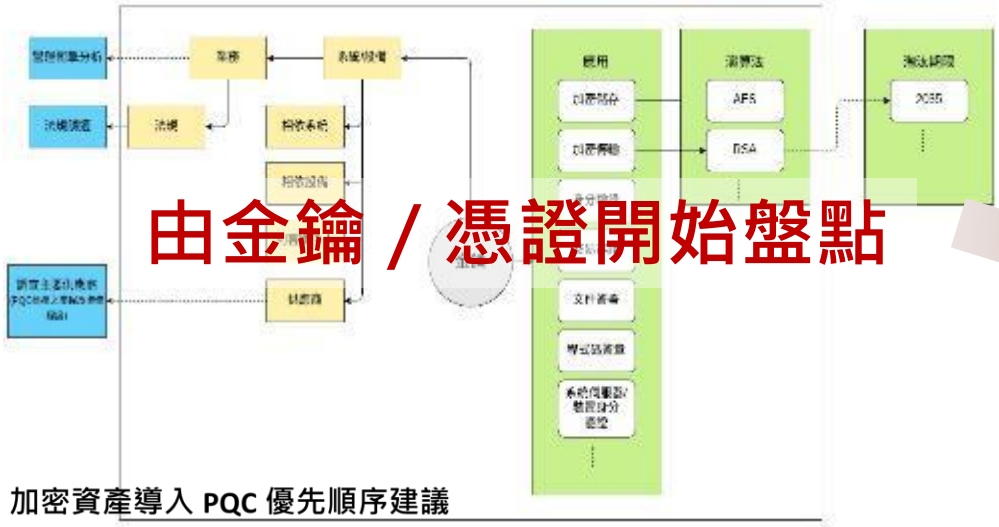
密碼資產初步盤點表 (參考金管會PQC先導計畫)

密碼資產：使用到密碼演算法的服務或資料。

法規	該業務金鑰管理需求的合規來源。
業務	使用該金鑰所支援的業務範疇。
應用	金鑰的用途：1.加密儲存,2.加密傳輸,3.身分驗證,4.交易存證,5.文件簽署,6.程式碼簽章,7.系統伺服器/裝置身分憑證
金鑰	組織維護的金鑰或憑證清單；若組織無相關紀錄，建議向配合之 PKI 業者取得。
金鑰長度	金鑰演算法之長度(位元數)。
演算法	(選單)金鑰採用的密碼演算法：
相依系統/服務	該系統或設備在密碼應用過程中所涉及或依賴的其他系統。
加密設備	該系統或設備在密碼應用過程中所涉及或依賴的其他設備。
供應商	相依介接系統/服務的供應商 or 加密所需服務/設備的供應商
負責單位	如:XX銀行系統部
備註	

Copyright of TWCA

盤點密碼資產 PQC READY程度 (參考金管會 PQC 先導計畫)

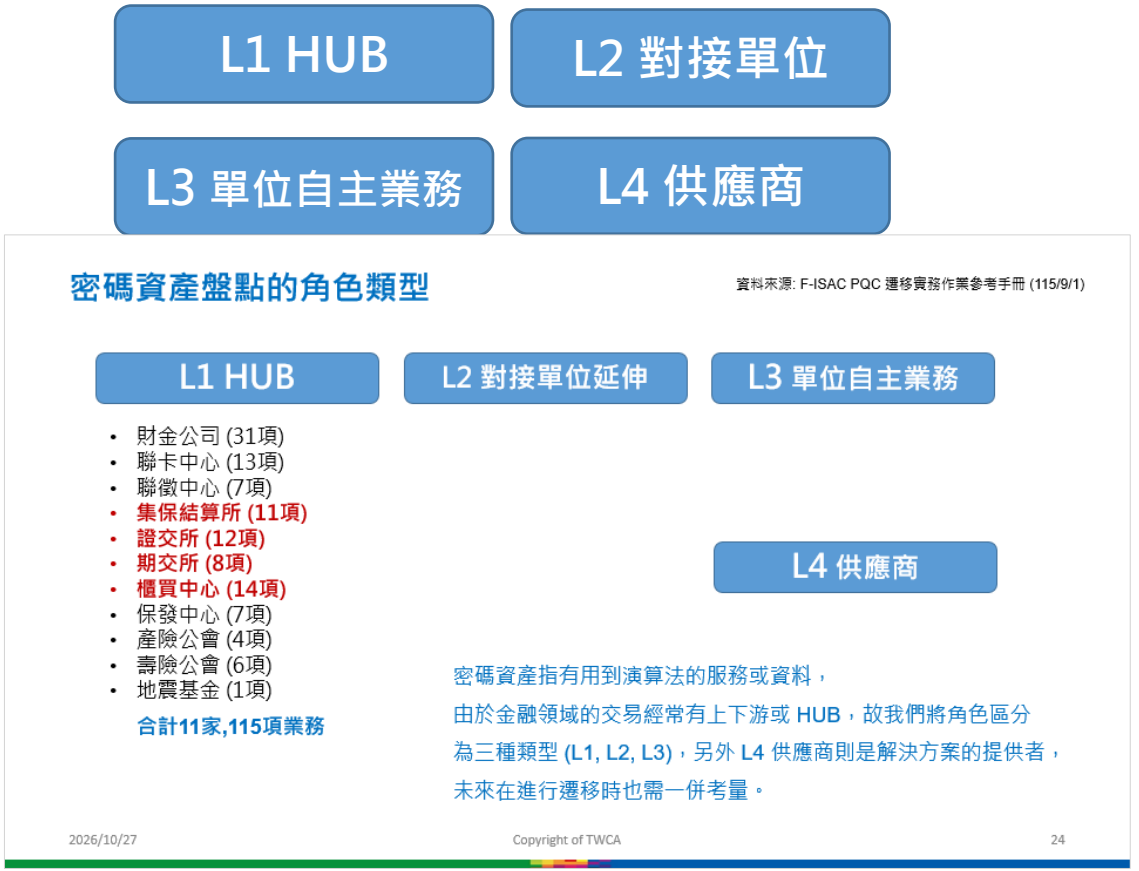


加密資產導入 PQC 優先順序建議

資料來源:NISA/ENISA/MAS/數發部,2025/8, TWCA整理

資產類型	分類面向	導入優先建議	服務
關鍵基礎建設	涉及金融穩定性、營運關鍵基礎設施的系統	優先（P0）—立即納入PQC規劃	金融交易中心,憑證機構(CA)
交易系統	高敏感度、高頻交易與外部暴露	優先（P0）—立即納入PQC規劃	FXML,EDI,股票下單
用戶身份驗證機制	使用者登入與身份驗證相關	優先（P0）—立即納入PQC規劃	Fast ID
長期保存的數位簽章文件	長效性（3年以上）保密性需求	高（P1）	電子保單
API與第三方介接通訊	對外連結風險與API供應鏈依賴	高（P1）	
內部資料庫加密與備份	內部資安韌性，涉及備份與恢復	中（P2）	
次要應用與非核心系統加密	低敏感度，風險影響較低的內部應用	低（P3）	

可再分別討論 P0 ,P1 ,P2 ,P3 的具體時程



Europol 金融服務 PQC 遷移優先順序矩陣

資料出處:2026 Quantum Safe Financial Forum (QSFF), Europol 2026

遷移時間分數

量子風險分數

	MT L1	MT L2	MT L3
QR L3	High (1) 立即進行	High (2) 近期規劃	High (3) 長期規劃
QR L2	Medium (4) 日常作業時處理	Medium (5) 追踪並處理	High (3) 長期規劃
QR L1	Low (6) 順帶處理	Low (6) 順帶處理	Low (6) 順帶處理

- 透過 **遷移時間** 及 **量子風險** 的雙重考量，決定後量子遷移優先順序。
- **量子風險** = 綜合考量（資料有效時間 + 曝露程度 + 影響嚴重度）
- **遷移時間** = 綜合考量（可用性 + 執行成本與時間 + 外部依賴性 ）

Copyright of TWCA

量子風險量化指標(QR) = 資料有效時間 + 曝露程度 + 影響嚴重度

量子風險等級 = （有效時間 + 曝露程度 + 影響嚴重度）÷ 3	
風險因子	**評量等級 (等級越高,表示風險越高)**
資料信任/有效時間 (SHELF LIFE)	• L1 = <2年 (short-term) • L2 = 2~5年 (medium-term) • L3 = >5年 (long-term)
曝露程度 (EXPOSURE)	• L1 = 資料僅限於自有基礎設施存取 • L2 = 資料存取僅限於特定的第三方 • L3 = 資料為公開可存取，或極易外洩
影響嚴重度 (SEVERITY)	• L1 = 影響微小，至多為聲譽影響 • L2 = 造成相關業務影響 • L3 = 造成嚴重中斷或重大影響

Copyright of TWCA

遷移時間量化指標(MT) = 可用性 + 執行成本與時間 + 外部依賴性

遷移時間量化指標 = ROUND (SUM OF Migration Time Factors Score / 3)	
遷移時間因子	評量等級 (等級越高,表示遷移時間越長)
解決方案可用性 (Solution Availability)	• L1 = 目前已可用，或預計於 1 年內推出 • L2 = 預計於 1 至 3 年內推出 • L3 = 時程不確定，或需 3 年以上
執行成本與時間 (Execution Cost and Time)	• L1 = 屬於日常營運（BAU）的一部分，僅需進行微調。 • L2 = 需要中度的架構變更。 • L3 = 需要重大、具不確定性或高昂成本的升級（例如：物流極其複雜的硬體更換）。
外部相依性 (External Dependencies)	• L1 = 依賴極低，或解決方案已被廣泛採用。 • L2 = 依賴第三方，且其轉型路線圖（Roadmap）明確為 1 至 3 年。 • L3 = 依賴第三方，但其轉型路線圖不確定或需 3 年以上。

- 通訊安全
- 加密保護
- 數位簽章

- 憑證體系
- 硬體&載具

遷移優先順序矩陣

資料出處:Quantum Safe Financial Forum (QSFF),2026

遷移時間分數

量子風險分數

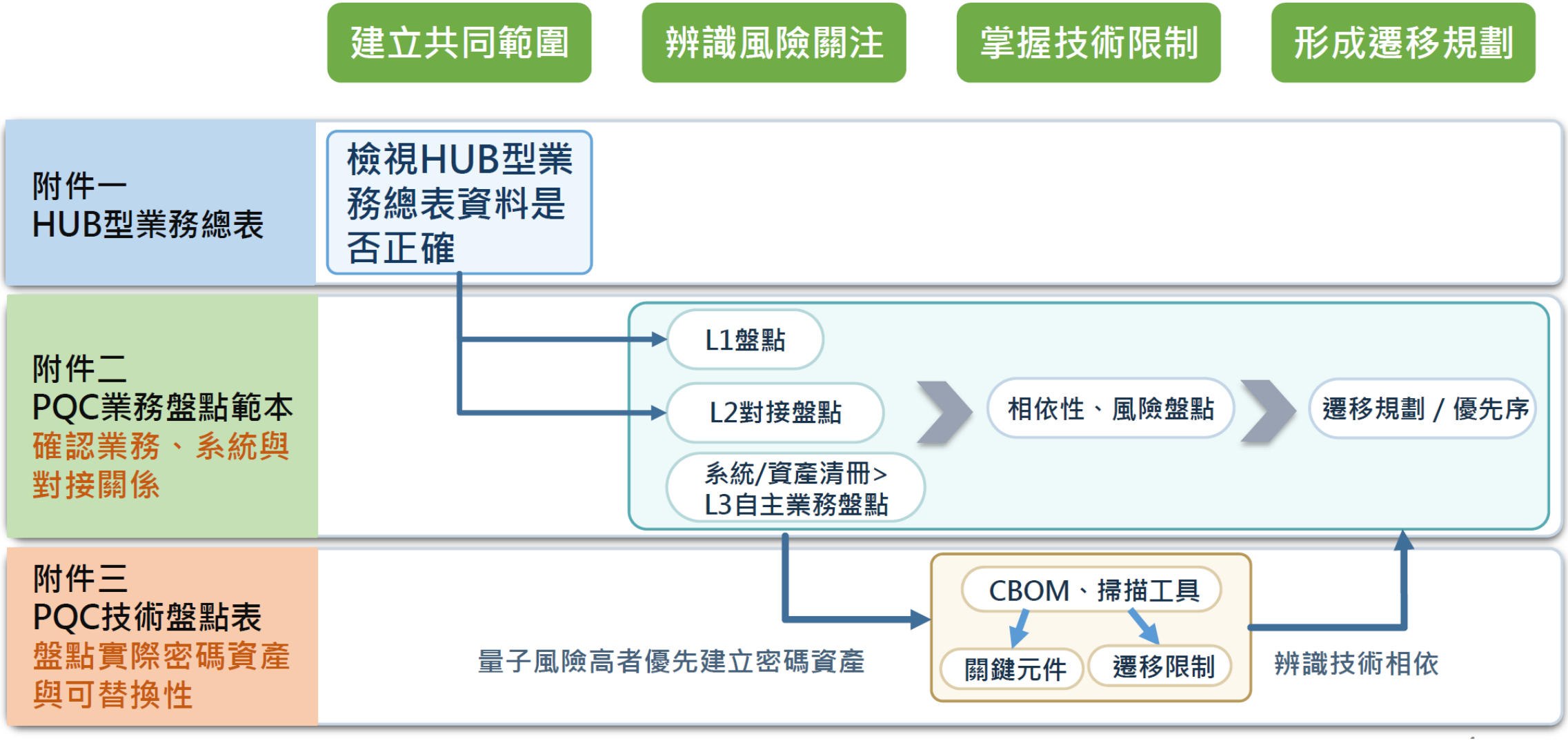
	MT L1	MT L2	MT L3
QR L3	High (1) 立即進行	High (2) 近期規劃	High (3) 長期規劃
QR L2	Medium (4) 日常作業時處理	Medium (5) 追踪並處理	High (3) 長期規劃
QR L1	Low (6) 順帶處理	Low (6) 順帶處理	Low (6) 順帶處理

- **高優先(紅色)：**
  1. 高風險+現成方案→立即進行
  2. 高風險+須準備工作→近期規劃
  3. 具長期仰賴關係的高風險與中風險→長期規劃。
- **中優先(黃色)：**
  4. 遷移路徑較短的中風險，可納入日常營運的升級計畫一併處理。
  5. 需規劃的中風險，應進行追踪，以確定最佳的準備時程。
- **低優先(綠色)：**
  6. 低風險應用案例：可藉由標準的系統現代化計畫，順帶尋求時機處理。

Copyright of TWCA

HUB 組織使用流程

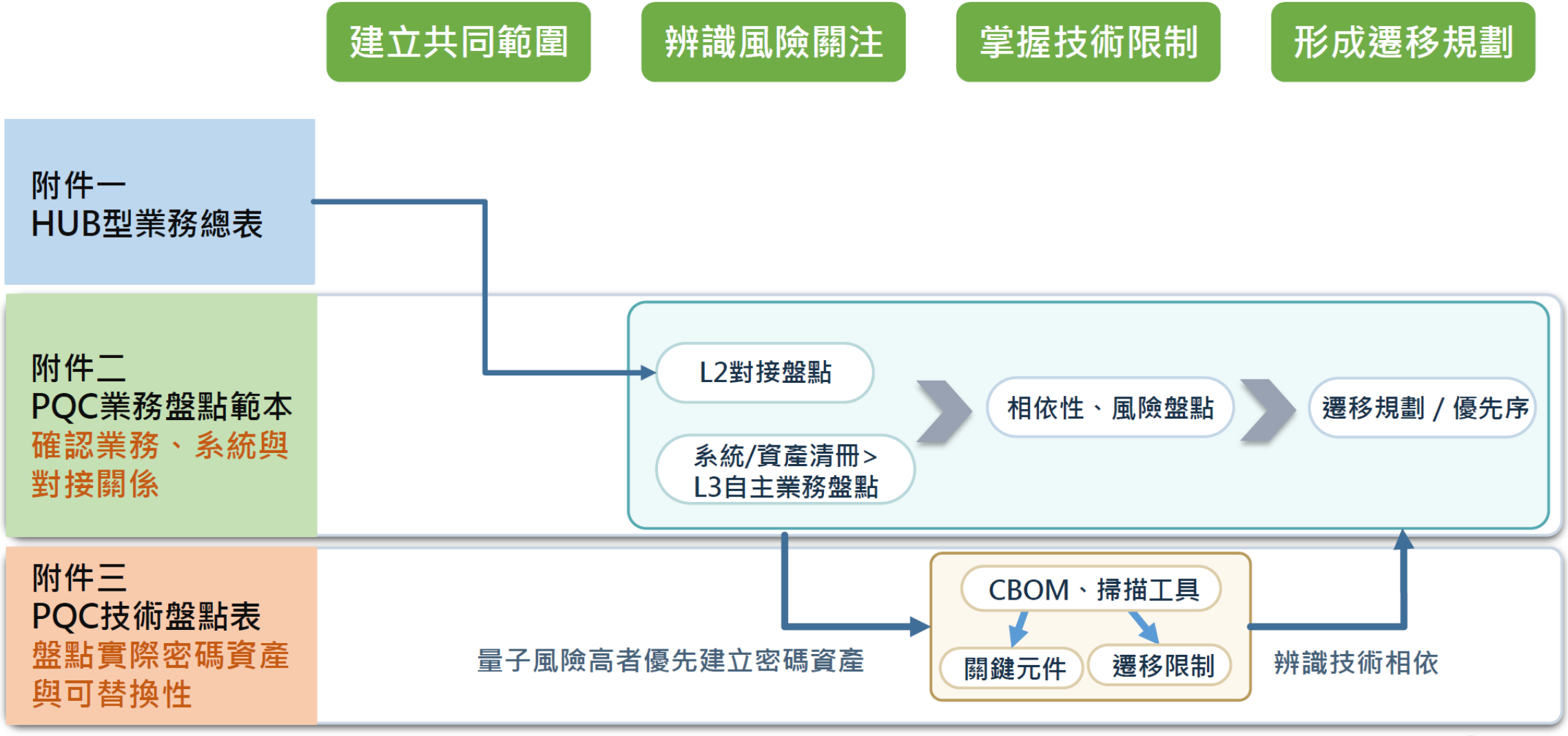
參考 F-ISAC PQC遷移實務作業參考手冊



Copyright of TWCA

非HUB 組織使用流程

參考 F-ISAC PQC遷移實務作業參考手冊



Copyright of TWCA

附件欄位關聯說明(範例)

參考 F-ISAC PQC遷移實務作業參考手冊

附件一、HUB型業務總表

項次	主導者	業務名稱	系統/設備名稱
FISC-01	財金公司	業務A	系統B

附件二、PQC業務盤點範本

盤點項次	盤點類型 (L1、L2、L3)	來源Hub業務項次	業務名稱	系統/設備名稱	密碼技術應用	資料/信任有效期間	暴露程度	遷移規劃/優先序	遷移群組
BANKA-0001	L2	**FISC-01**	存款帳戶即時轉帳	核心帳務系統	傳輸加密、訊息驗證、身分驗證	2至5年	中	依Hub時程辦理	FISC-MG-01

附件三、PQC技術盤點表

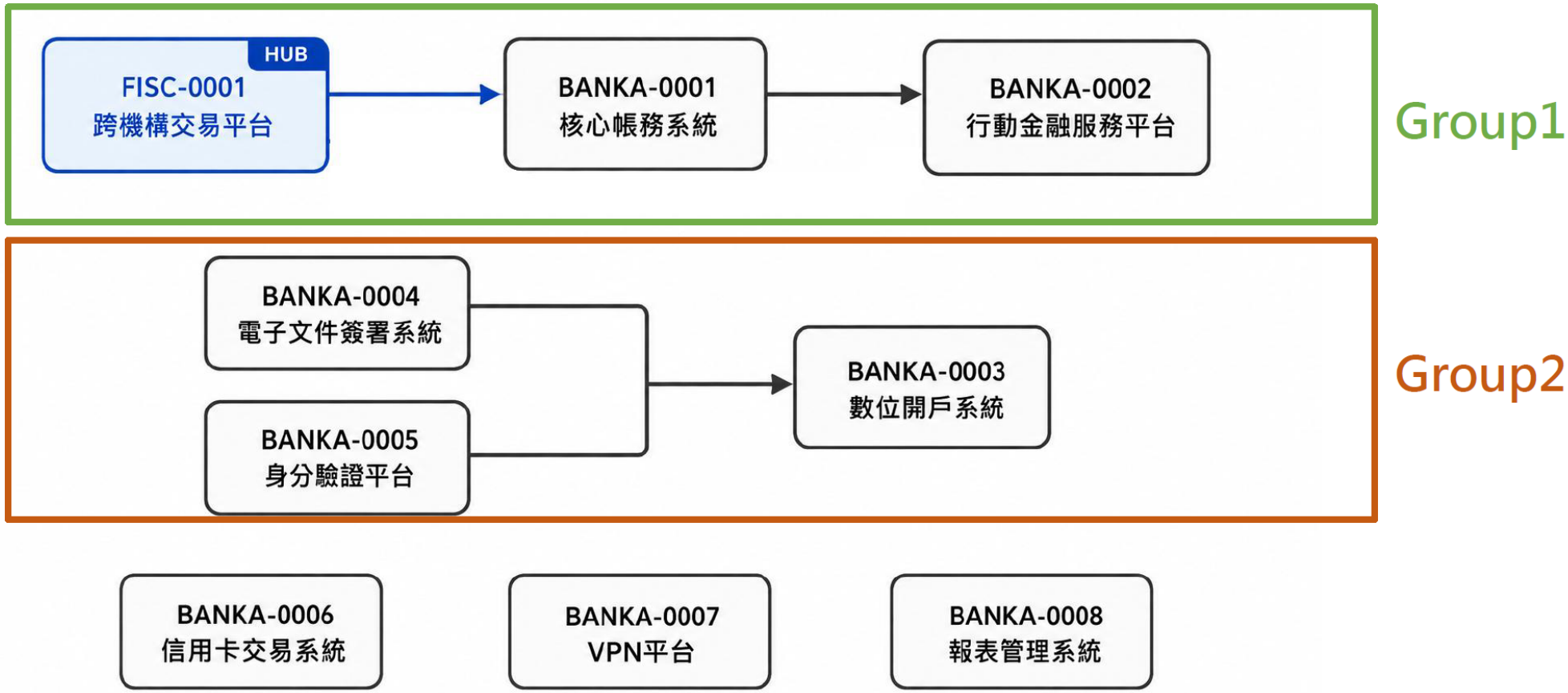
技術項次	來源業務盤點項次	密碼用途	協定 / 演算法	PQC追蹤需求
BANKA-TECH-0002	**BANKA-0001**	數位簽章 / 驗證	RSA-3072 / RSA-PSS	需追蹤
BANKA-TECH-0003	**BANKA-0001**	對稱加密	AES-256-GCM	不需追蹤

Copyright of TWCA

附件二、PQC業務盤點範本(續)

參考 F-ISAC PQC遷移實務作業參考手冊

遷移相依性盤點



Copyright of TWCA

金融實務五大面向與主管機關政策時程



Copyright of TWCA

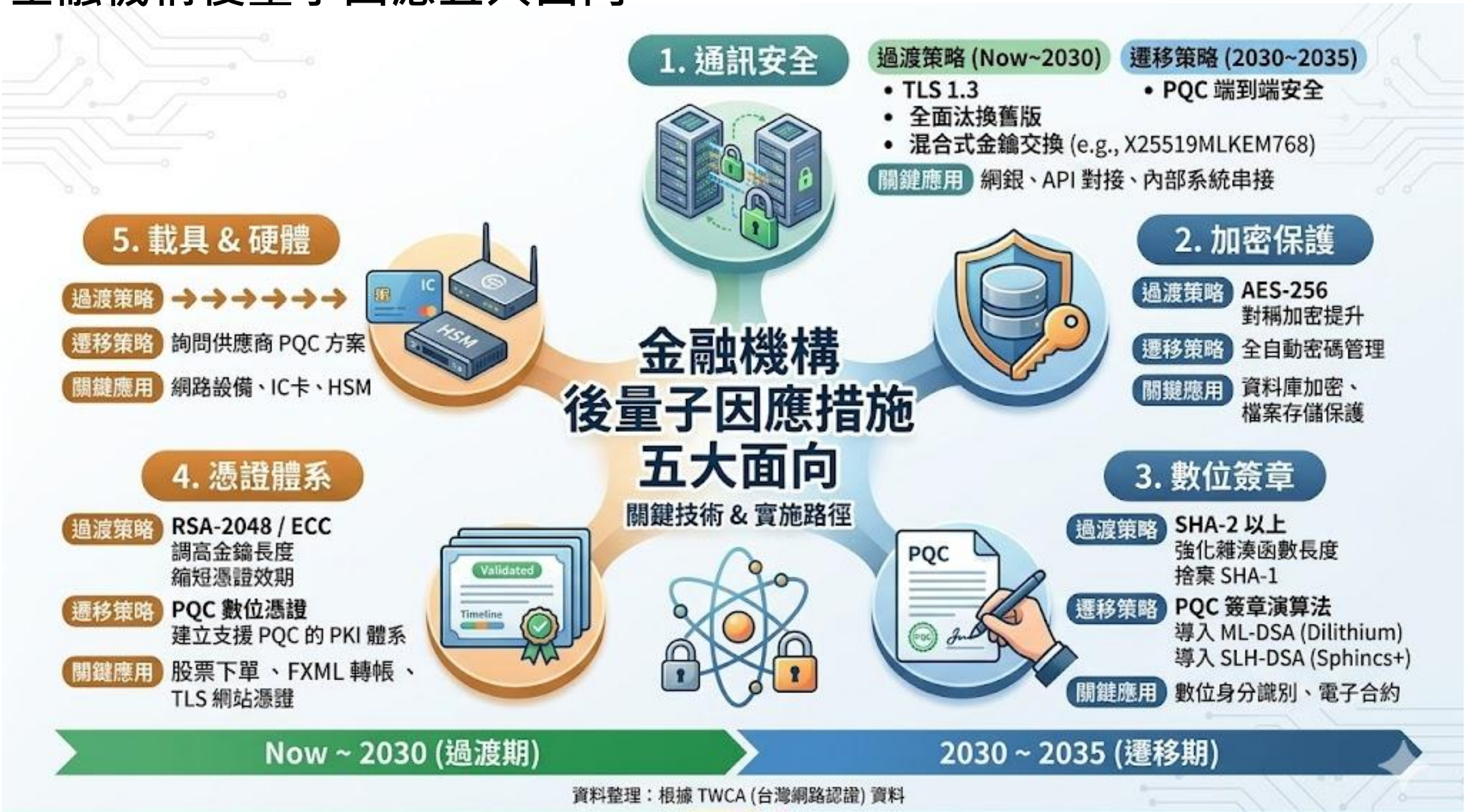
金管會後量子遷移時程規劃

資料出處:金管會後量子遷移白皮書 (2026/6/18)

階段	建議時程	重點工作
準備與規劃	2025–2026	● 建立治理架構與盤點方法。 ● 盤點對外TLS端點與關鍵PKI/CLM/KMS/HSM。 ● 建立CBOM黃金資料來源。 ● 啟動供應鏈準備度治理與採購文件更新。 ● 建立測試案例與版本基準雛形。 ● 逐步提升既有演算法至安全性較高的演算法(如3DES升級為AES 256、SHA 1升級為SHA 2) 。
試辦與基礎升級	2027–2029	● 選定可控情境進行PoC / 試辦。 ● 測試混合模式（Hybrid Mode），評估對交易延遲與硬體效能的衝擊。 ● 提升TLS 1.3覆蓋率並清理反密碼模式。 ● 導入或強化憑證自動化與金鑰治理。 ● 建立切換與回退演練。 ● 開始建立跨機構共同測試窗口。
優先遷移（高風險/高關鍵）	2029–2032	● 依量子風險評分與外部互通窗口，優先推動對外通路、跨機構介接、關鍵驗章/簽章與高敏感長效期資料之遷移。 ● 導入PQC或混合模式並完成端到端測試；同步處置「卡關元件」汰換。
全面遷移與收斂	2032–2035	● 擴大至剩餘中低風險情境與長尾系統。 ● 完成跨體系PKI與信任鏈一致化。 ● 針對需LTV之既有存證/歸檔資料完成分期處置。 ● 建立常態化的演算法迭代與例行升級流程。

Copyright of TWCA

金融機構後量子因應五大面向



資料整理：根據 TWCA (台灣網路認證) 資料

金融機構 後量子因應措施五大面向

關鍵面向	演進策略 (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

Copyright of TWCA

支援 PQC 的瀏覽器版本

重要的網站入口建議即早因應，採用支援 PQC 的版本

- Default for Chrome 131+ ↗
- Default for Edge 131+ ↗
- Default for Safari 26+ ↗
  - System-wide support in iOS 26, macOS Tahoe 26, and other Apple operating systems ↗

- Firefox 132+
- Chrome 131+
- Edge 131+
- 這幾個大概去年底發布
- Safari 26是最近發布

資料出處: https://developers.cloudflare.com/ssl/post-quantum-cryptography/pqc-support/, updated at 2025/10/28

PQC 金鑰和簽章值大小的預估

資料出處: https://www.ndss-symposium.org/ndss-paper/post-quantum-authentication-in-tls-1-3-a-performance-study/, 2025/7/9 擷取,作者整理

加密強度

傳統電腦

量子電腦

傳統

後量子

Algorithm	Public Key Size (Bytes)	Private Key Size (Bytes)	Signature Size (Bytes)	Classical Security Level	PQ Security Level
RSA 2048	256 (數學)	256 (數學	256 (modulus)	112 bits	~0 bits
RSA 3072	384 (數學	384 (數學)	384 (modulus)	128 bits	~0 bits
RSA 4096	512 (數學	512 (數學	512 (modulus)	152 bits	~0 bits
ECDSA P-256	33 (壓縮)	32 (scalar)	64	128 bits	~0 bits
ECDSA P-384	49 (壓縮)	48 (scalar)	96	192 bits	~0 bits
ECDSA P-521	67 (壓縮)	66 (scalar)	132	256 bits	~0 bits
Dilithium II	1184	2800	2044	100 bits	91 bits
Dilithium IV	1760	3856	3366	174 bits	158 bits
Falcon 512	897	1281	690	114 bits	103 bits
Falcon 1024	1793	2305	1330	230 bits	230 bits
SPHINCS+ SHA256-128f-simple	32	64	16976	128 bits	64 bits

Copyright of TWCA

JOSE 及 FIDO 對後量子的準備現況

- JOSE (JSON Object Signing and Encryption) Framework



JOSE 的基礎規範尚未具備 PQC 能力，但 IETF 已積極準備中。

於 2024 年 1 月發布 **白皮書**
”Addressing FIDO Alliance’s Technologies in Post Quantum World”

FIDO 目前尚未公佈 PQC 規格。

資料出處: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://fidoalliance.org/wp-content/uploads/2024/04/FIDO-BTC-White-Paper_FIDO-Alliance-and-Post-Quantum-Cryptography.pdf,2024/1

乙太坊後量子防護架構 (預計 2029達成)

共識層與合約升級

EIP-8394 驗證存款合約

- 擺脫單一的 BLS 簽名演算法
- 支援「可變長度」與「多種密碼學」方案
- 允許「新舊驗證機制」並存，並預留未來可透過共識投票淘汰舊 BLS 驗證機制

架構重整與效能壓縮

Lean Ethereum + leanXMSS + zkVM

- Lean Ethereum (架構精實)
- LeanXMSS (基於雜湊的新型簽名方案)
- zkVM (零知識虛擬機)：進行 250 倍的資料壓縮，將現有合約內容進行壓縮成一個小的 Proof。

帳戶層面彈性切換

EIP-8141 彈性切換方案

- 支援終端用戶自主升級
- 不強制改變用戶地址
- 平滑過渡至量子安全架構

比特幣 (Bitcoin)：拉鋸中

Copyright of TWCA

公有鏈 vs. 聯盟鏈：後量子升級策略比較表

比較維度	公有鏈（Permissionless）（例如：以太坊、比特幣）	聯盟鏈（Permissioned）
網路屬性	去中心化、全球匿名散戶參與、無單一管理者。	封閉或半封閉、節點為受信任的金融或企業機構。
升級驅動力	必須依賴**全網硬分叉**或引入**帳戶抽象**，協調成本極高。	可由**聯盟管理者發起**，透過統一的軟體版本更新與時程規劃執行。
對「用戶/客戶」的影響	用戶需自行升級錢包或遷移資產（如從 EOA 轉至智慧合約錢包）。	一般用戶（如保戶）無感，完全由後端保險公司節點處理。
歷史資料與資產處理	處理歷史公鑰暴露和沈睡資產（如中本聰幣）極具爭議，動輒面臨社群分裂。	可透過**歷史檢查點重新簽署、金鑰輪替或鏈下封存歸檔**輕鬆解決，無共識分裂風險。
策略建議	雙軌並行與模組化壓縮 • 共識層預先佈局 • 技術瘦身與壓縮 • 用戶端平滑過渡	管理者協調，節點同步升級，歷史歸檔 • 統一時間表升級 • 歷史資料封存與重新錨定 • 企業節點金鑰升級

Copyright of TWCA



結論與證期業者行動呼籲

Copyright of TWCA

密碼資產盤點的原則及作法



快篩

- 全面及簡單



問診

- 細部盤點
- 遷移優先順序評估



關鍵資產檢查

- CBOM（外部工具或廠商提供）
- 供應商協助

Copyright of TWCA

Europol 金融服務 PQC 遷移優先順序矩陣

資料出處:2026 Quantum Safe Financial Forum (QSFF), Europol 2026

遷移時間分數

量子風險分數	MT L1	MT L2	MT L3
QR L3	High (1) 立即進行	High (2) 近期規劃	High (3) 長期規劃
QR L2	Medium (4) 日常作業時處理	Medium (5) 追踪並處理	High (3) 長期規劃
QR L1	Low (6) 順帶處理	Low (6) 順帶處理	Low (6) 順帶處理

- 透過 **遷移時間** 及 **量子風險** 的雙重考量，決定後量子遷移優先順序。
- **量子風險** = 綜合考量（資料有效時間 + 曝露程度 + 影響嚴重度）
- **遷移時間** = 綜合考量（可用性 + 執行成本與時間 + 外部依賴性 ）

Copyright of TWCA

密碼資產初步盤點表 (參考金管會PQC先導計畫)

密碼資產：使用到密碼演算法的服務或資料。

法規	該業務金鑰管理需求的合規來源。
業務	使用該金鑰所支援的業務範疇。
應用	金鑰的用途：1.加密儲存,2.加密傳輸,3.身分驗證,4.交易存證,5.文件簽署,6.程式碼簽章,7.系統伺服器/裝置身分憑證
金鑰	組織維護的金鑰或憑證清單；若組織無相關紀錄，建議向配合之 PKI 業者取得。
金鑰長度	金鑰演算法之長度(位元數)。
演算法	(選單)金鑰採用的密碼演算法：
相依系統/服務	該系統或設備在密碼應用過程中所涉及或依賴的其他系統。
加密設備	該系統或設備在密碼應用過程中所涉及或依賴的其他設備。
供應商	相依介接系統/服務的供應商 or 加密所需服務/設備的供應商
負責單位	如:XX銀行系統部
備註	

Copyright of TWCA

證券商受影響的場景，建議由五大面向尋求解決方案

- 受影響的範圍

場景	優先辦理			待 CA	待供應商
	通訊	**加密**	**簽章**	**憑證/金鑰**	**硬體載具**
會員帳號密碼	O	O			
網站主機的 TLS 憑證	O	O		O	
客戶和主機的通訊加密 (https, ftps等)	O	O			
下單憑證			O	O	
長效期資料防護 (數位簽章 + 金鑰加密)	O	O	O	O	O
通訊設備 (如: VPN)	O	O			O
金鑰儲存設備 (如: HSM)		O		O	O
主管機關的交易及資料傳輸	依 L1 主管機關各業務的規劃時程配合辦理				

Copyright of TWCA

金融機構 後量子因應措施五大面向

關鍵面向	演進策略 (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&金鑰	**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、FIDO驗證、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

Copyright of TWCA

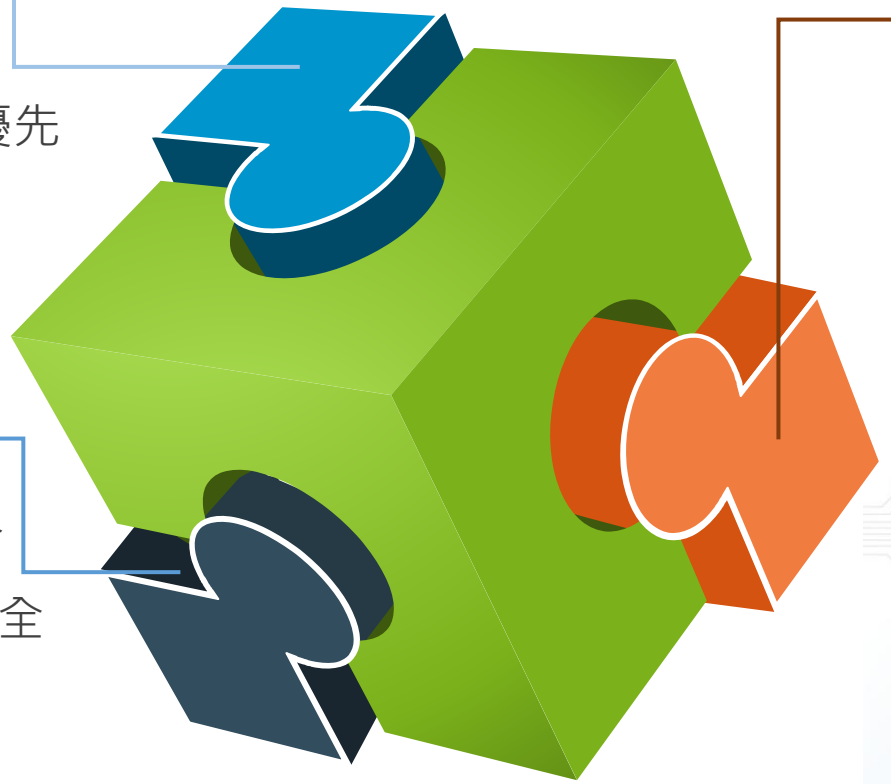
結論

盤點密碼資產

- 盤點密碼資產。
- 參考遷移優先順序矩陣列出優先順序。

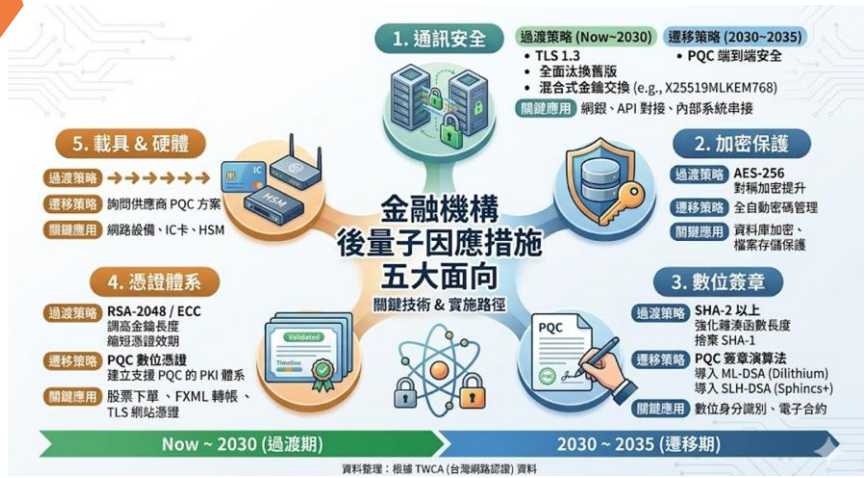
訂定 時程及策略

- 因應**策略**：演進策略 / 遷移策略
- **時程**：準備期/試辦期/優先遷移/全面遷移。



由5大關鍵面向 規劃加密轉型與韌性提升

- 由通訊安全, 加密保護, 數位簽章, 憑證體系, 載具 & 硬體 五個關鍵面向，規劃實施措施。



Copyright of TWCA



Copyright of TWCA