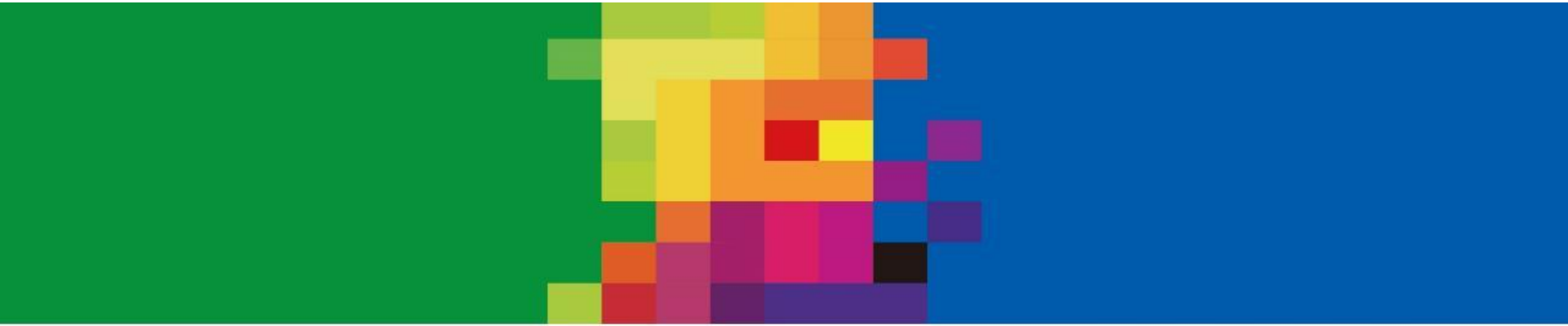
證交所專題演講
後量子因應對策

TWCA 策略發展部協理 連子清



TWCA 臺灣網路認證

TWID 身分識別中心

WHAT
什麼是量子電腦？

量子 是一種物理領域的突破

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

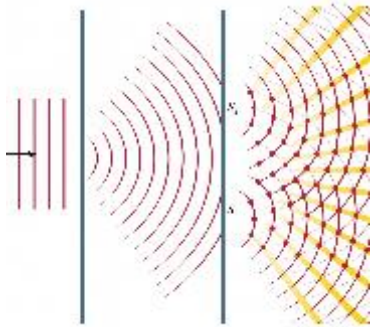
- 與傳統的物理狀態在某一時間只有一個特定狀態不同，量子狀態可以在同一時間具有不同的狀態。

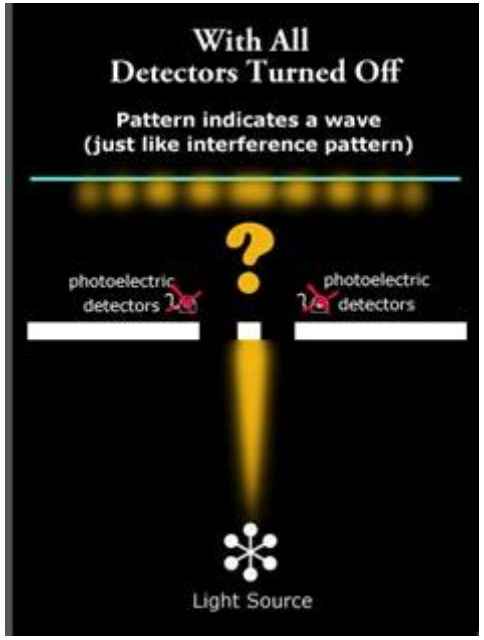
量子糾纏 (Entanglement)　不管多遠都牽連在一起

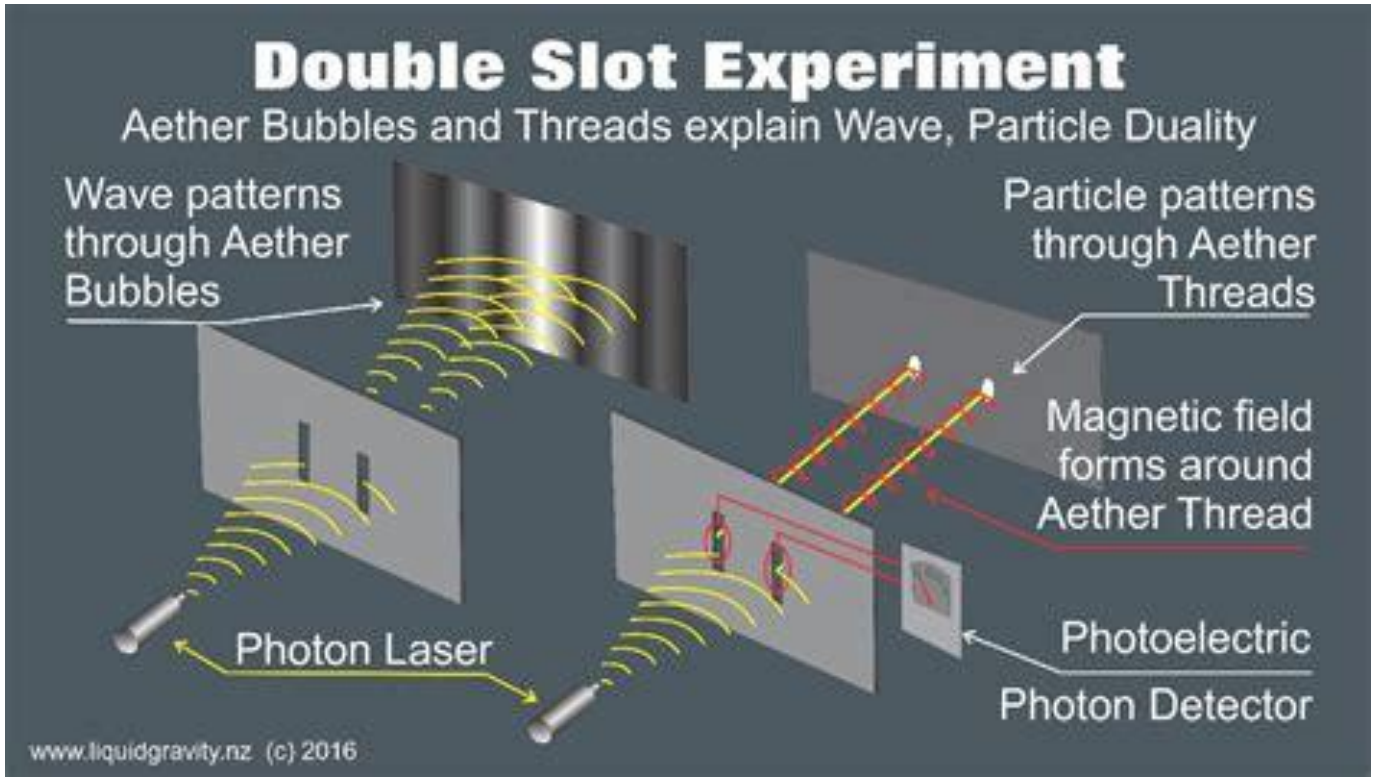
- 兩個或多個粒子的量子狀態相互連接的量子力學現象，使得一個粒子的狀態立即與另一個粒子的狀態相連，無論它們之間的距離有多遠。

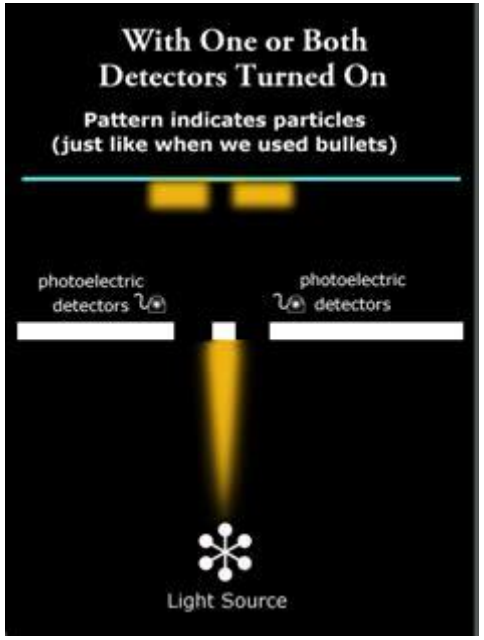
雙縫實驗

光是粒子還是波動？









左圖：沒偵測器，光是波

右圖：有偵測器，光是粒子

量子電腦及量子晶片

CRQC（Cryptanalytically Relevant Quantum Computer）

指的是一種足以威脅現代加密系統安全性的量子電腦。具有實際破解主流加密演算法能力的量子運算平台。

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。

WHY
為什麼我們要
因應量子威脅？

量子電腦的演算法及對加密的威脅

因為量子電腦的運算方式與傳統電腦根本不同，傳統演算法不是沒效率就是直接失效，所以量子電腦發展出新的演算法。

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。

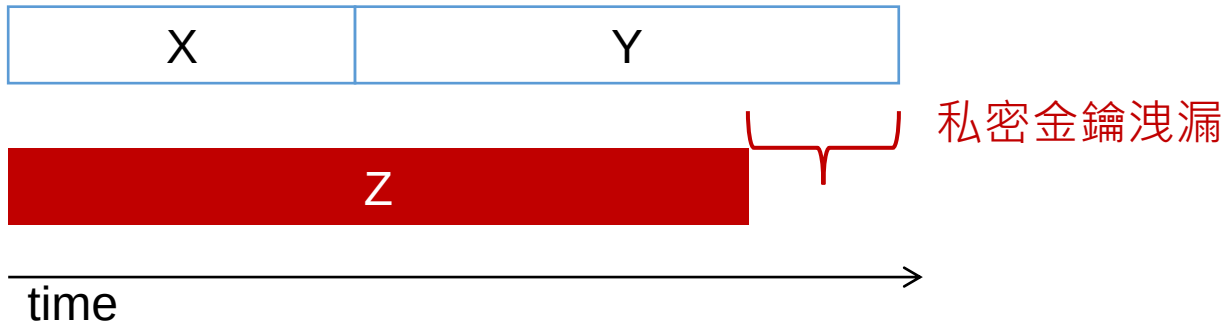
量子電腦 對 非對稱式演算法 的威脅 > 對稱式演算法

先保存 後破解

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



不同演算法常運用領域

應用領域	對稱式加密 (效能高/加密大量資料)	非對稱式加密 (身分驗證/交換金鑰)	常用演算法
資料保存 (靜態加密)	V		AES-256
自然人憑證 / 數位簽章		V	RSA, SHA
金融憑證		V	RSA,SHA
TLS 網站通訊 (HTTPS)	**V (資料傳輸)**	**V (身分握手)**	AES (對稱), RSA/ECC (非對稱)
晶片金融卡	V		AES (取代舊有的 3DES)
通訊加密 (如 LINE/Signal)	V	V	AES, X25519 (非對稱金鑰交換)
區塊鏈 (錢包與交易)		V	ECC (Secp256k1), EdDSA

雖然量子電腦對非對稱式加密威脅較大，
但實務上，對稱式加密應用的領域範圍較廣（如：**資料保存**及**網站通訊**），影響不容忽視。
特別是**資料保存**，通常具一定保存期限，更易受到先保存後破解的威脅。

WHEN
什麼時侯
量子威脅會到來？

Y2Q 威脅：破解主流加密所需的量子算力

根據學術界和產業的估計，若要運行 Shor's Algorithm 來破解主流加密，需要達到以下標準：

破解 RSA 2048 加密

- 所需「邏輯量子位元」：
  - 估計約需要 **1,000 到 2,000 個** 高質量、低錯誤率 的邏輯量子位元（Q buit)。(註：邏輯量子位元是經過錯誤校正的穩定量子位元)
  - 所需「物理量子位元」：由於目前的物理量子位元錯誤率高，每個邏輯量子位元需要數百甚至數千個物理量子位元來進行錯誤校正。因此，總共需要的物理量子位元數量可能高達 數百萬個。

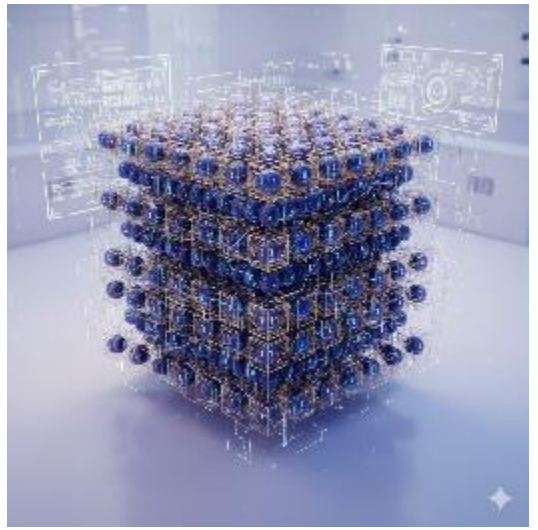
破解 ECC 加密（如 256 位元）

- 所需邏輯量子位元數量可能比 RSA 略少，但同樣需要 **數千個** 邏輯量子位元。

廠商的目標與現實差距

「數百個物理量子位元」

Now → **Y2Q 時間預估**



「數千個高保真度、錯誤率極低的邏輯量子位元」

現在的進展與目標數量仍有顯著差距：

- 目前的物理量子位元數量：頂尖廠商（如 IBM）已經實現了數百個物理量子位元的處理器（例如 133 ~ 433 個 Qubits）。
- 目前的邏輯量子位元數量：目前世界上能夠實現的邏輯量子位元數量非常少，通常還在個位數到十位數的驗證階段。

Y2Q Clock

許多專家和機構對 Y2Q 的預測範圍很廣：

- **相對保守預測**：2035 年至 2045 年。
- **較激進預測**：最早可能在 2030 年代初（約 2033 年）達到破解規模。

能在量子計算下存活的密碼系統，稱為 “後(抗)量子密碼系統”

PQC: Post-Quantum Cryptography

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 適用產生金鑰及加密, 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
- 2025 年 7 月
  - **金管會推動 PQC 先導小組**
- **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。

目前公佈的 PQC 演算法

NIST 在 2024/8/13 公佈了三項 PQC 演算法標準

項目	對應算法	用途/類型
FIPS 203	ML-KEM (previously CRYSTALS-Kyber)	金鑰封裝（Key-Encapsulation）
FIPS 204	ML-DSA (previously CRYSTALS-Dilithium)	數位簽章
FIPS 205	SLH-DSA (SPHINCS+)	無狀態雜湊簽章
FIPS 206 (預定)	FN-DSA (FALCON)	數位簽章
HQC（2025 新增）	Hamming Quasi-Cyclic	金鑰封裝（Key-Encapsulation），備援

CNSA 2.0 演算法要求

General Purpose Algorithms

Algorithm	Function	Specification	Parameters	
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
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.	金鑰封裝及通訊加密
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.	非對稱加密及簽章

HOW
如何因應
量子威脅？

對抗

用量子電腦對抗量子威脅

遷移

採用後量子演算法

過渡

傳統/後量子並行或串聯

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

CA/Browser Forum 對後量子的政策

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

現有演算法

過渡 (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)

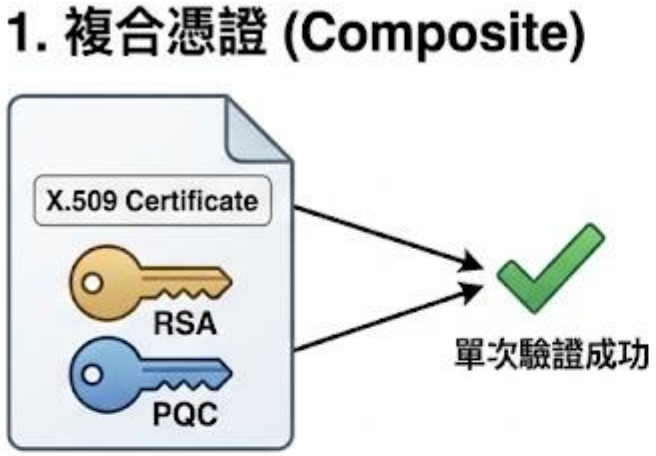
後量子 (PQC)

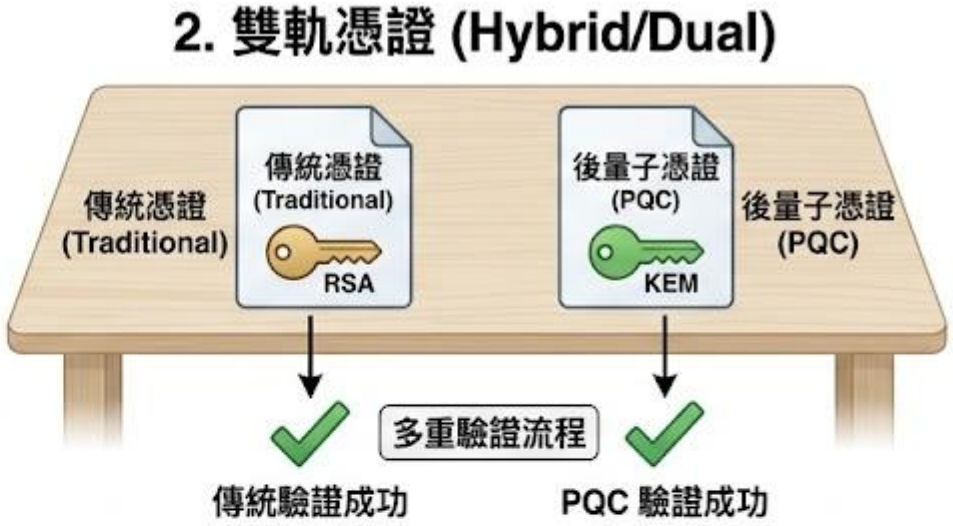
- ✓ 目前 X.509 規格已公佈對 PQC 演算法的支援
- ☐ 瀏覽器支援作法 (討論中)
- ☐ 硬體支援 (如:IC卡,HSM均在認證中)

摘要自 CA/B Forum 2026/3

常見的過渡作法

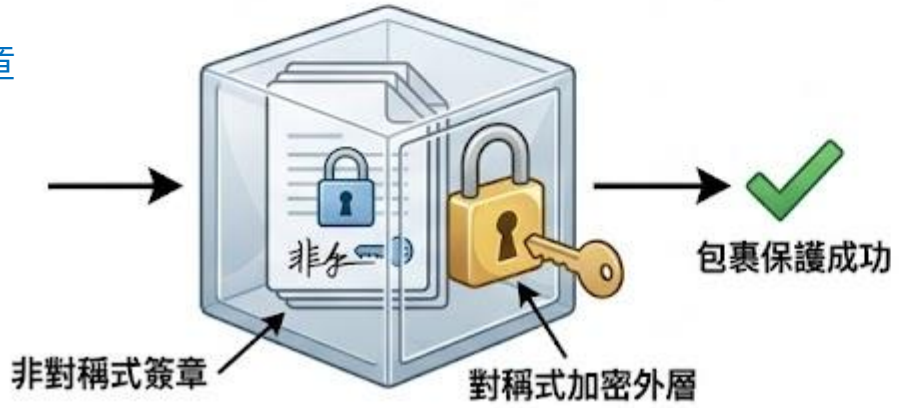
一張憑證同時具備傳統及 PQC 金鑰及簽章

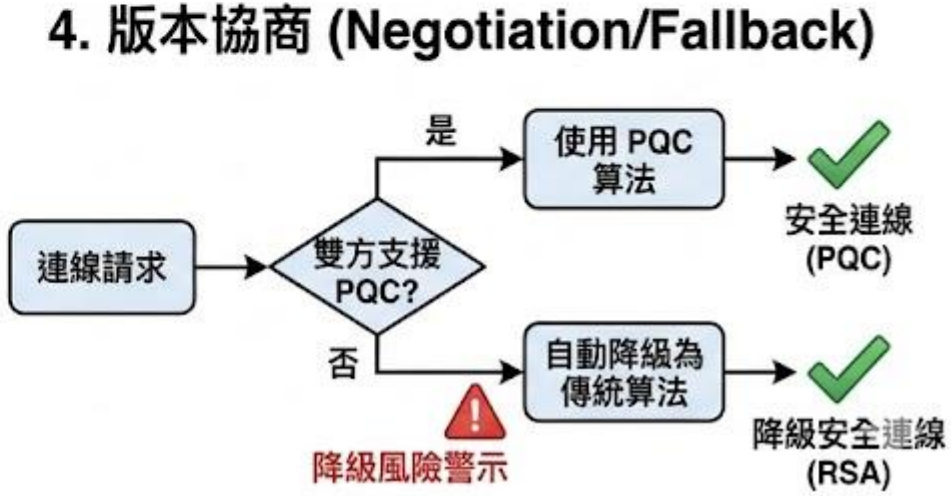




兩張憑證分別具備傳統及 PQC 金鑰及簽章

非對稱式簽章+外層對稱式加密





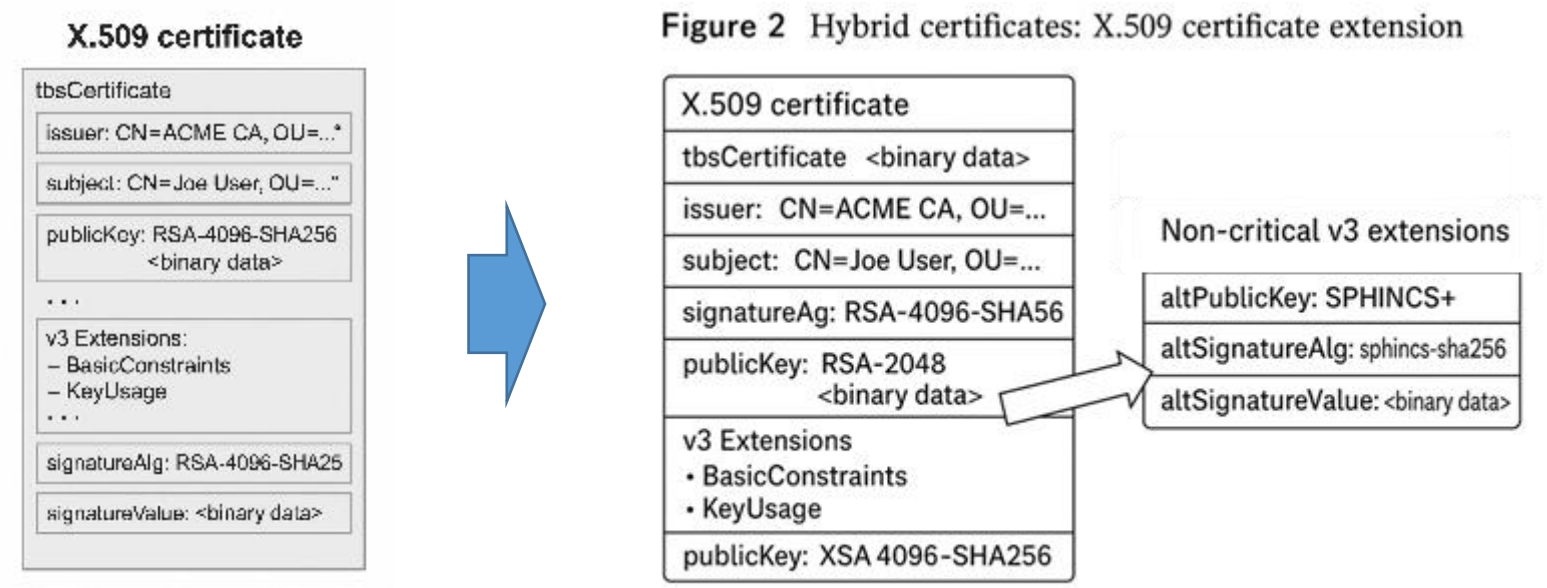
依版本自動支援 PQC 或降級

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. 過渡	**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**	**建立「加密敏捷性」的底座**
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 "**過渡**" 和 "**遷移**" 是業界目前最常採用策略。

利用 X.509 延伸欄位實現 複合式憑證



優點:

- 無縫且安全過渡到 PQC
- 強化安全性(運用雙層保護)
- 彈性部署

缺點:

- 影響效能
- 須考慮互通性 (新舊系統之間)
- 管理複雜度高 (可能須 CLM 以協助管理)

資料出處: https://securityboulevard.com/2024/07/preparing-for-the-quantum-leap-with-hybrid-certificates/?utm_source=chatgpt.com, 擷取日期:2025/4/22

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

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

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

NIST PQC 標準化過程制定的安全等級

Cat 2 & 4 為過渡等級，後來都跳過。

類別	對應對稱安全強度	對應傳統公鑰等價	含義
Category 1 (Cat 1)	≥ AES-128 的安全強度	ECC P-256 (~128-bit) / RSA-3072	如果有人能破解此演算法，就能破解 AES-128，安全基準線。
Category 3 (Cat 3)	≥ AES-192 的安全強度	ECC P-384 (~192-bit) / RSA-7680	適合需要更高安全壽命的系統（如長期憑證、金融核心系統）。
Category 5 (Cat 5)	≥ AES-256 的安全強度	ECC P-521 (~256-bit) / RSA-15360	最高安全等級，對應頂級長期敏感應用（軍事、國家安全、CA 根憑證）。

金融機構後量子遷移建議

由密碼資產重要性切入→按資產特性

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	涉及用戶資料與高風險行為驗證	優先（P0）—立即納入PQC規劃	金融 Fast ID
長期保存的數位簽章文件	長效性（5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

密碼資產盤點的角色類型

L1 HUB

- 財金公司
- 聯徵中心
- 集保結算所
- 證交所
- 期交所
- 保發中心
- 壽險公會

L2 對接單位

- 臺灣銀行
  - 金融卡發卡系統

L3 單位自主業務

- 臺灣銀行
  - ATM自動櫃員機

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)，未來在進行遷移時也需一併考量。

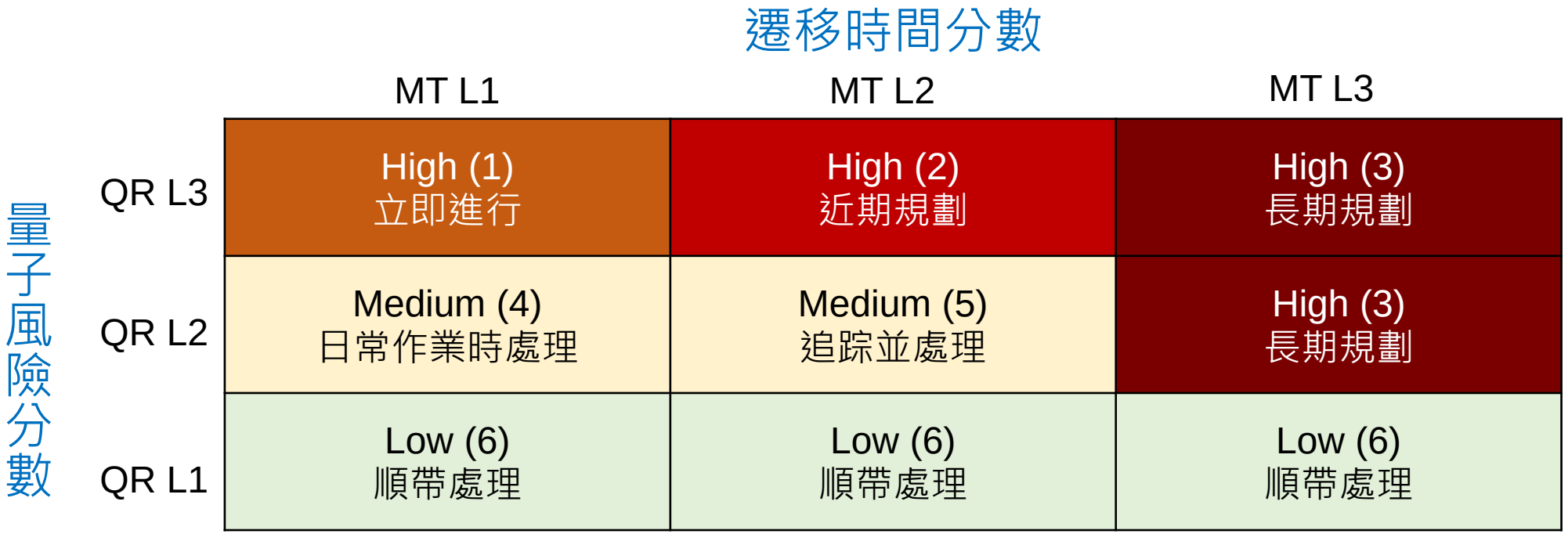
密碼資產初步盤點表 (參考金管會PQC先導計畫草案內容，進行中)

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	

遷移優先順序矩陣

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



- 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 (資料保存時間 + 資料敏感度 + 曝漏程度)
- **遷移時間** = 綜合考量 (可用性 + 執行成本與時間 + 外部依賴性)

量子風險量化指標 = 資料保存時間 + 資料敏感度 + 曝漏程度

量子風險等級 = ROUND (SUM OF Quantum Risk Factors Score/ 3)	
風險因子	評量等級 (等級越高,表示風險越高)
資料保存時間 (SHELF LIFE)	• L1 = <2年 (short-term) • L2 = 2~5年 (medium-term) • L3 = >5年 (long-term)
資料敏感度 (SEVERITY)	• L1 = 影響微小（僅限於聲譽影響） • L2 = 顯著業務影響 • L3 = 嚴重營運中斷
曝漏程度 (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

遷移時間量化指標 = 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 = 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）。
外部依賴程度 (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。

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。

金融機構後量子遷移時程表

2025 ~ 2026

準備與規劃

資產盤點、建立 CBOM、既有算法升級至 AES-256。

2027 ~ 2029

試辦與基礎升級

PoC 試辦、混合模式測試、TLS 1.3 普及化。

2029 ~ 2032

優先遷移

高風險系統導入 PQC、執行端到端完整測試。

2032 ~ 2035

全面遷移

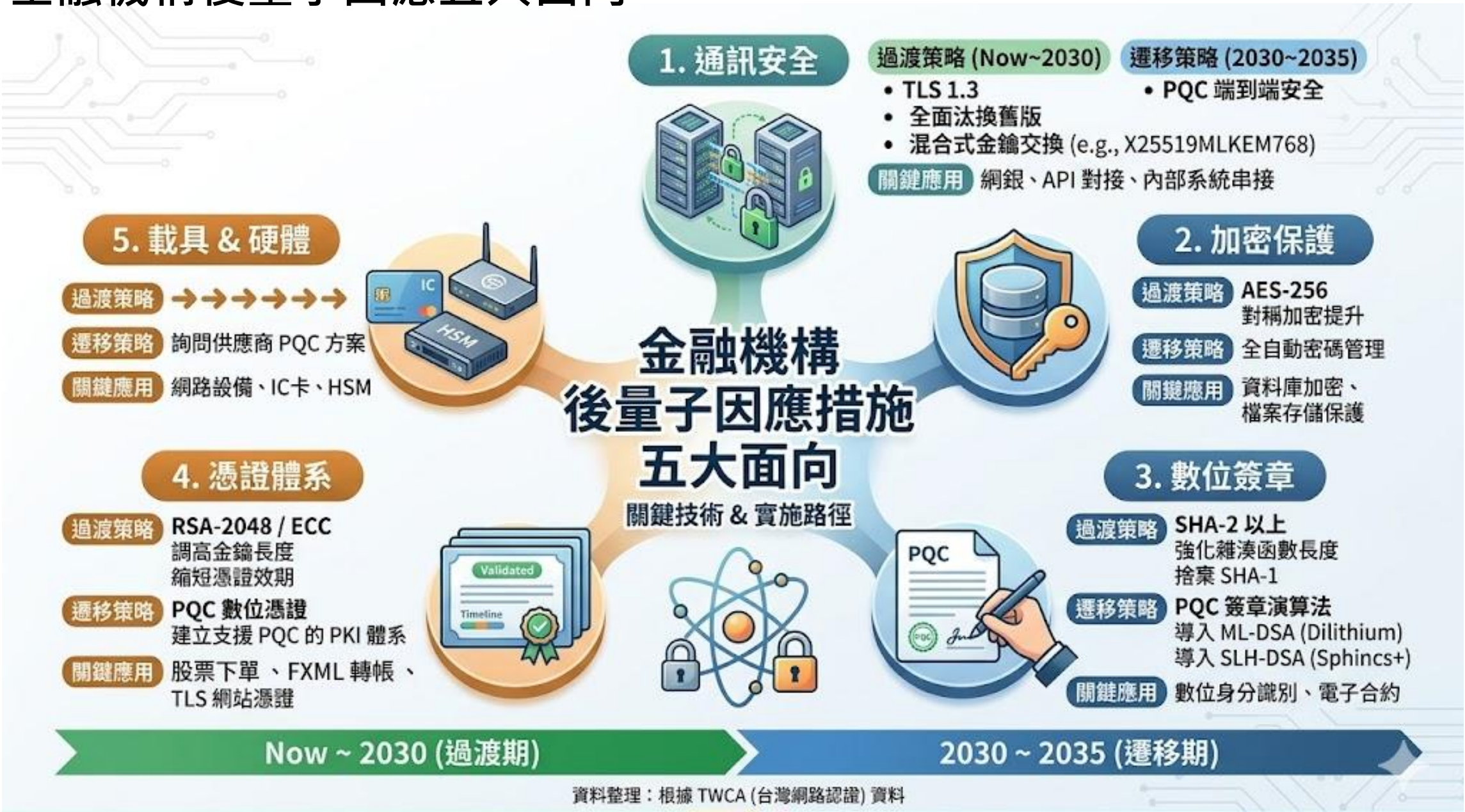
全體系佈署完成、收斂密碼資產、建立迭代流程。

金管會後量子遷移時程

資料來源:參考金管會後量子遷移草案，實際內容請依金管會正式公告為準。

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。

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	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		網銀、API 對接、內部系統串接。
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、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。	股票下單、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

6

結論與建議

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

- 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（資料保存時間 + 資料敏感度 + 曝漏程度）
- **遷移時間** = 綜合考量（可用性 + 執行成本與時間 + 外部依賴性 ）

證期市場 因應量子威脅的建議方案

- 立即盤點密碼資產（使用到密碼演算法的服務或資料）
- 過渡 和 遷移 並行，依盤點結果分階段導入
  - 過渡方案 (可運作至2029)
    - 雜湊函數 提升（SHA 2 以上)
    - 對稱加密 提升 (AES 256 bits)
    - 非對稱簽章 RSA 2048 以上
  - 遷移方案 (自2029建議開始導入)
    - 雜湊函數提升至 SHA-3
    - 通訊加密 強制 TLS 1.3 with PQC
    - 非對稱加密及簽章 更換 PQC

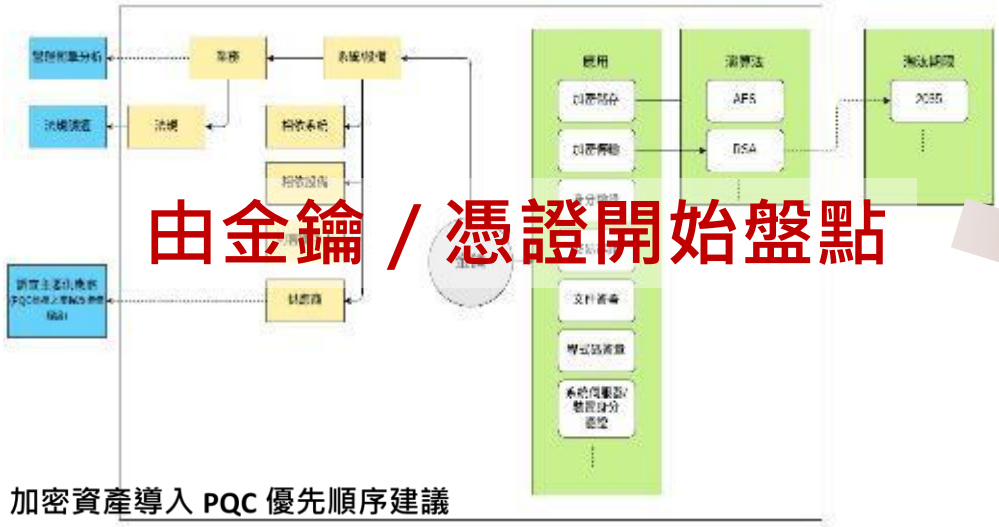
建議方案	建議時間
盤點密碼資產	立即進行
雜湊函數提升至SHA 2	Now~2026
通訊加密 提升 • 支援 TLS 1.3 • 強制 TLS 1.3 with PQC	 Now Now~2029
對稱加密 (AES 256 bits)	Now~2029 (依資料保存期限)
證期下單憑證及簽章 support PQC	配合主管機關規劃

金管會後量子遷移時程

資料來源:參考金管會後量子遷移草案，實際內容請依金管會正式公告為準。

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。

結論1：評估密碼資產導入 PQC (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[illegible]為[illegible]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（5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

由金鑰 / 憑證開始盤點

由業務特性開始盤點

L1 HUB　L2 對接單位　L3 單位自主業務

密碼資產初步盤點表 (參考金管會PQC先導計畫草案內容，進行中)

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	

2026/5/7　Copyright of TWCA　31

結論2：延緩量子威脅的準備工作

通訊加密

- 傳輸層：提升至 TLS 1.3，並確認支援 PQC。
- TLS 網站憑證：先盤點目前部署的設備或主機，以及連線單位（註明本身為 Client 或 Server），待 CA 廠商提供。
- 網站設備：詢問 設備及主機供應商，能否支援 PQC？

演算法

- **採對稱式**建議提升至 AES 256 bits，**非對稱式**建議提升至 RSA 2048 bits，**雜湊函數**建議提升至 SHA 2。

HSM

- 詢問供應商產品如何支援PQC：FIPS 140-3 Level 3，CAVP 加解密演算法驗證服務（已可申請），或加解密模組(CMVP，目前還未開放申請）

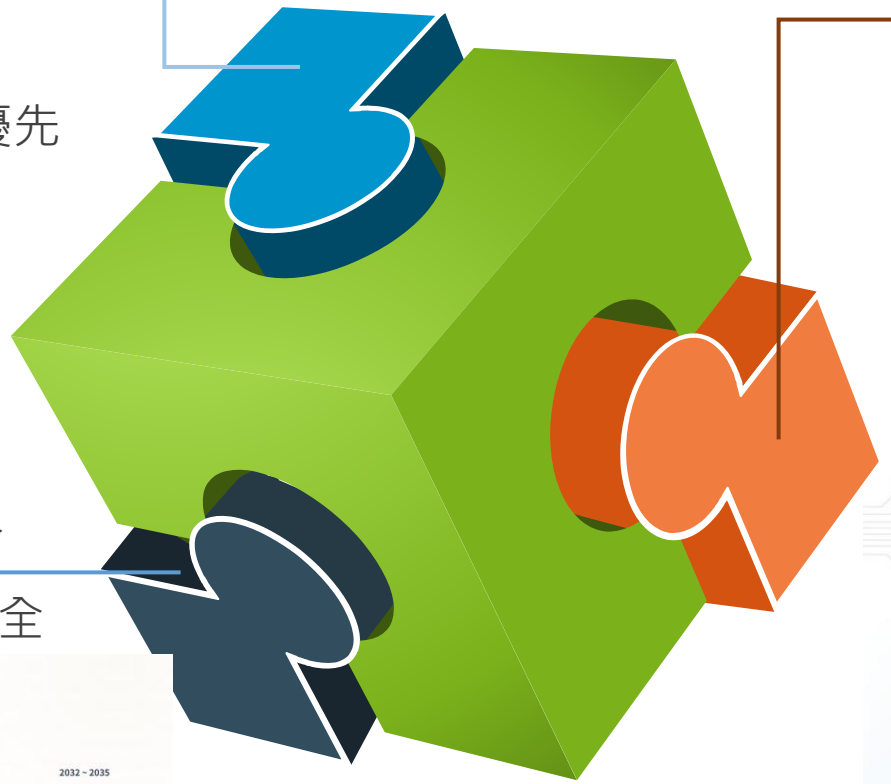
結論與呼籲

評估及列出 遷移優先順序

- 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**：過渡策略 / 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。