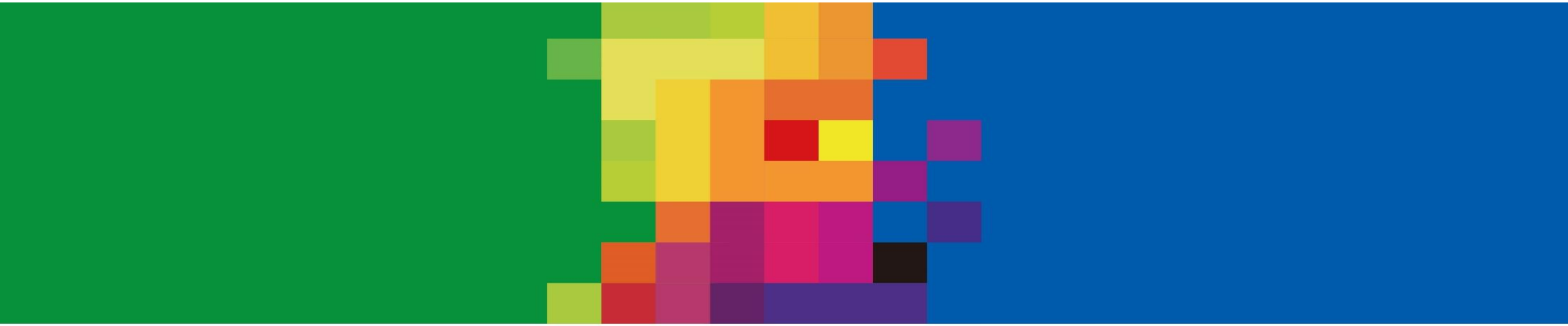
金融業的 量子挑戰 與 後量子密碼 (PQC) 因應策略

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

PQC 的 4W1H

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。

量子電腦及量子晶片

CRQC（Cryptanalytically Relevant Quantum Computer）

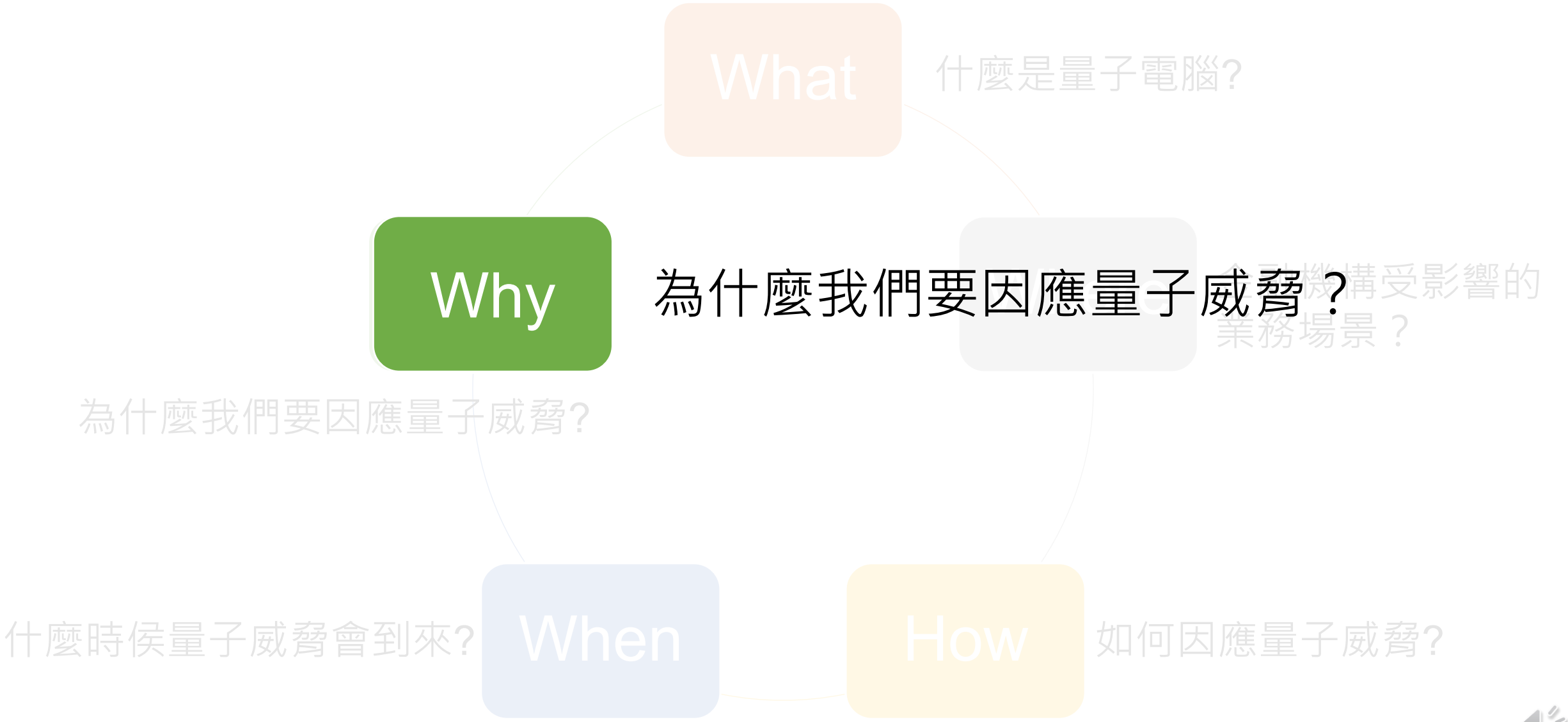
指的是一種足以威脅現代加密系統安全性的量子電腦。具有實際破解主流加密演算法能力的量子運算平台。

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。

PQC 的 4W1H



為什麼我們要因應量子威脅？

量子電腦對加密的威脅

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，所以必須發展新的演算法，才能在量子環境下正確又安全地運作

- 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，因此支撐非對稱加密的「難解性」會被量子電腦徹底打破。
- 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。

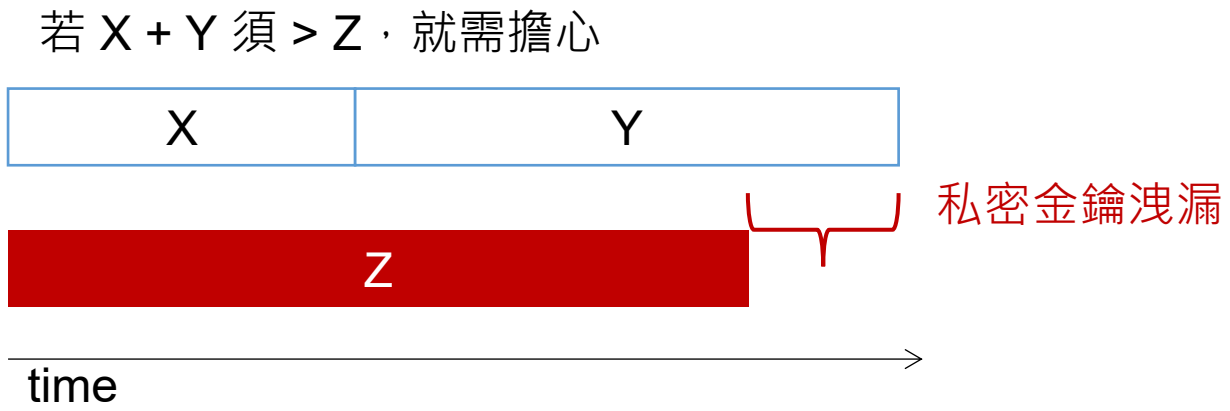
- 對稱加密：Grover's Algorithm（葛羅佛演算法）
- 葛羅佛演算法可用於加速暴力破解：
  - 原本需嘗試 2^n 才能找到密鑰；
  - 現在只需約 $2^{\frac{n}{2}}$ 次。
- 影響：
  - 意味著 256-bit AES 的等效安全性在量子下為約 128-bit；仍具實際安全性，只需加長密鑰即可抵抗量子攻擊。

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**」
憑證信任體系崩壞	根據 RSA 或 ECC 所建立的信任鏈（PKI）將完全失效。

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



PQC 的 4W1H

What 什麼是量子電腦?

Who 金融機構受影響的業務場景？

When 什麼時侯量子威脅會到來？

Why 為什麼我們要因應量子威脅?

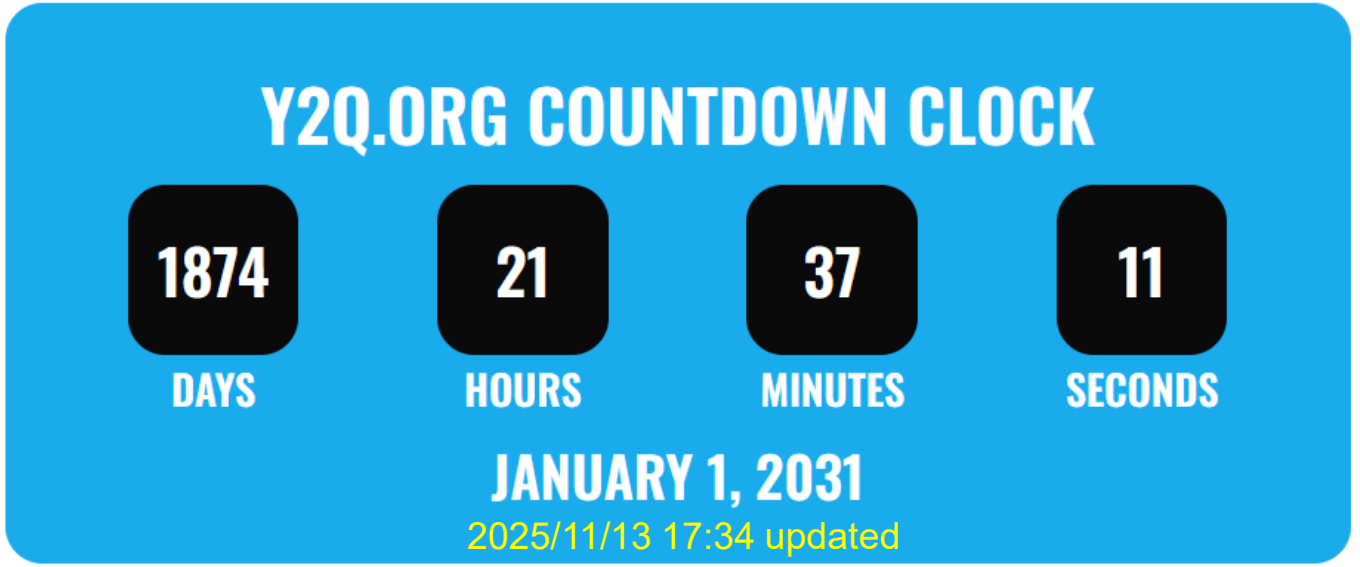
When 什麼時侯量子威脅會到來?

How 如何因應量子威脅?

Y2Q Clock

量子計算 源自物理領域的突破，它正在改變我們對運算能力的想像。

後量子密碼系統 為了應對量子計算可能帶來的威脅應運而生。主要是透過數學方法的加強，能夠在現有的環境中直接部署與執行。

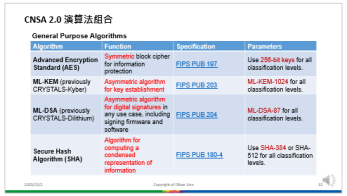


能在量子計算下存活的密碼系統，稱為“後(抗)量子密碼系統”

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）


CNSA 2.0 演算法組合

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.
ML-KEM (previously CRYSTALS-Kyber)	Asymmetric algorithm for key establishment	FIPS PUB 203	ML-KEM-1024 for all classification levels.
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.
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.

- 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
- **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。

- IETF **憑證規格**結合後量子(已於 2025/10 發佈)
- FIPS **將後量子納入 FIPS 140-3** (目前 CAVP 已可接受申請,CMVP 預計 2025 年底可能開始接受申請)

這二件事將影響 CA 遷移至後量子的啟動時間。

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 演算法組合

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.
ML-KEM (previously CRYSTALS-Kyber)	Asymmetric algorithm for key establishment	FIPS PUB 203	ML-KEM-1024 for all classification levels.
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.
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.

PQC 的 4W1H

What 什麼是量子電腦?

Where 金融機構受影響的業務場景？

How 為什麼我們要因應量子威脅?

When 什麼時侯量子威脅會到來?

How 如何因應量子威脅?

如何因應量子威脅？

- 國際對 量子電腦威脅 的建議與因應
- CA, Browser, FIDO 等技術的準備狀態及態度

國際對 量子電腦威脅 的建議與因應

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

可以用量子電腦來對抗量子攻擊嗎？

- **設備不夠理想**
  - 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 (Authentication)：**
  - 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。
- **成本與整合**
  - QKD 設備成本太高
- **拒絕服務攻擊 (Denial-of-Service, DoS)**
  - 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

歐美安全主管機關對 量子技術 的因應態度

特點	ENISA (歐洲網路與資訊安全局)	NSA (美國國家安全局)
總體立場	**積極推動與整合**，視為未來網路安全策略的重要組成部分。	**高度謹慎**，不推薦在國家安全系統中使用，除非克服限制。
主要關注點	• 推進歐盟量子戰略，實踐試點應用，制定認證標準， • 與現有的網路安全政策（如 NIS2 指令，希望提高整個歐盟的網路安全水準）保持一致。	評估 QKD 的技術限制、成本效益和易用性，更偏好 PQC。
與 PQC 關係	**互補，同時發展 QKD 和 PQC。**	**偏好 PQC**，認為其是更可行且高效的替代方案。
對 DoS 的看法	意識到 DoS 風險，但在實際應用中探索緩解方案。	認為 DoS 是一個顯著的脆弱性，影響其可靠性。

QKD (Quantum Key Distribution)：量子金鑰分配

PQC (Post-Quantum Cryptography)：後量子密碼學

CA/Browser Forum 對後量子的看法

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 **過渡** 的作法。

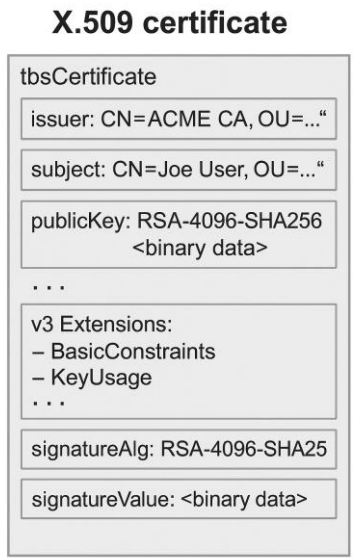
目前 國際 CA 組織尚未確認對 PQC 的政策

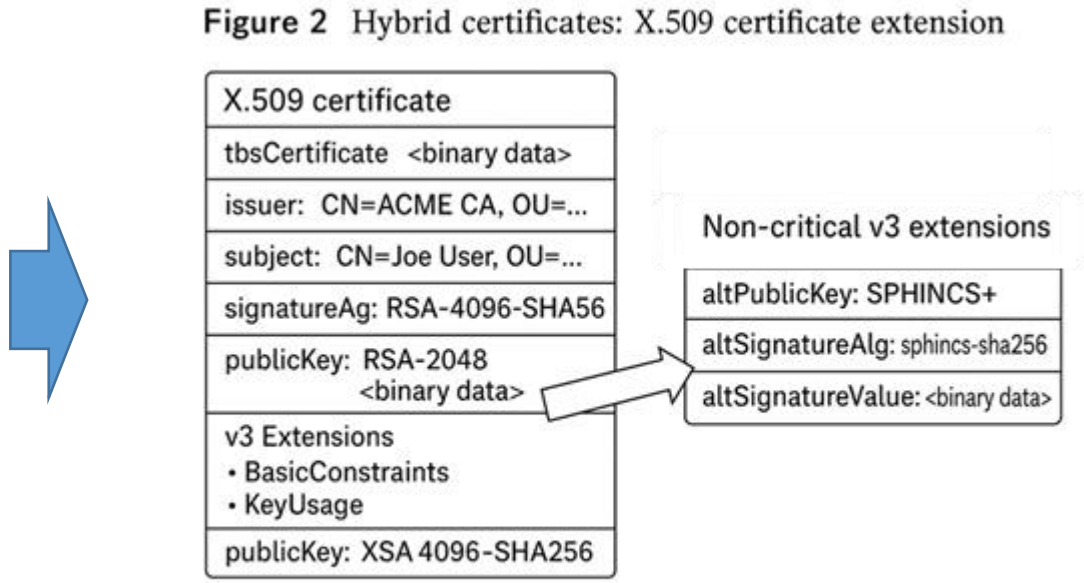
摘要自 CA/B Forum Tokyo 2025/3

過渡作法

項目	Hybrid（混合式）	Composite（複合式）
英文	TWO Certification Path : Hybrid Certificates	ONE Certification Path : Composite Certificates
結構	**兩張獨立憑證 / 兩組金鑰**	**單一憑證**，內含多組金鑰與簽章
信任鏈 (Chain)	**兩條獨立信任鏈**	**單一信任鏈**
驗證方式	驗證兩張憑證、兩組簽章（可選其一）	所有簽章**都要驗證通過**才算有效
相容性	✅ 與現有 PKI 相容性高	⚠️ 舊設備與程式需支援解析複合憑證格式
安全保證模式	提供過渡選擇，若其中一條路徑弱化仍有另一條備援	強一致性驗證（若任一簽章失敗就視為無效）
管理複雜度	高（需維護兩套金鑰、CSR、OCSP、CRL 等）	低（單一憑證管理流程）
實作狀態	較成熟（如 Entrust、Google Cloud 均有支援）	標準化進行中（IETF 草案推動中）

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

瀏覽器支援 TLS 1.3 一覽表

建議金融業及政府網站以 Modern 版本為最低要求

Configuration	Firefox	Android	Chrome	Edge	Internet Explorer	Java	OpenSSL	Opera	Safari
Modern	63	10.0	70	75	--	11	1.1.1	57	12.1
Intermediate	27	4.4.2	31	12	11 (Win7)	8u31	1.0.1	20	9
Old	1	2.3	1	12	8 (WinXP)	6	0.9.8	5	1

- **Modern**: Modern clients that support TLS 1.3, with no need for backwards compatibility
- **Intermediate**: Recommended configuration for a general-purpose server
- **Old**: Services accessed by very old clients or libraries, such as Internet Explorer 8 (Windows XP), Java 6, or OpenSSL 0.9.8

資料出處: https://wiki.mozilla.org/Security/Server_Side_TLS, updated at 2025/10/28

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

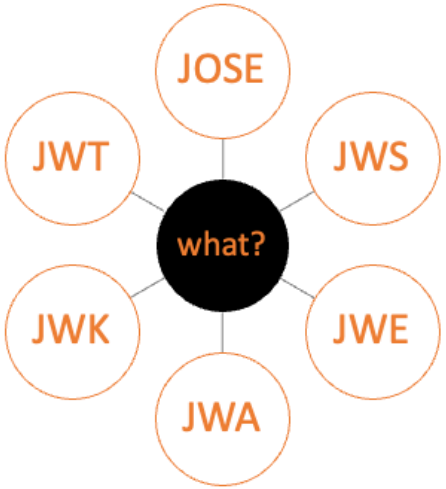
- Default for Chrome 131+ ↗
- Default for Safari 26+ ↗
  - System-wide support in iOS 26, macOS Tahoe 26, and other Apple operating systems ↗
- Default for Edge 131+ ↗

- 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

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

後量子

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）。

PQC 的 4W1H

Where

金融機構受影響的業務場景？（Impact on Finance）

- 密碼資產盤點建議(依金鑰/憑證或資產重要性)
- 通訊加密/憑證盤點建議

不同組織 對 密碼資產導入 PQC 評估面向之建議

參考 NIST (美國國家標準與技術研究院), ENISA (歐盟網路與資訊安全局), MAS (新加坡金融管理局) 及數發部，對密碼資產導入 PQC 之優先順序評估面向，整理如下表。

評估面向	來源機構	說明
1. 資料保存壽命 (Data Longevity / 資產壽命)	NIST、ENISA、MAS、數發部	涉及長期 (>5年) 保密性需求的資產，風險暴露期較長，應優先導入 PQC。
2. 資訊敏感度 (Data Sensitivity)	NIST、MAS、數發部	涉及個資、交易紀錄、高機密資料的系統，應被標示為高風險且優先轉換。
3. 系統對外暴露面 (Exposure Level)	ENISA、MAS、數發部	面向外部網路、第三方、政府或企業資訊流通的系統，風險暴露高，需優先納入 PQC 計畫。
4. 涉及關鍵基礎建設 (Critical Infrastructure)	數發部、MAS	涉及金融穩定性、營運關鍵基礎設施的系統，發生資安事件將產生重大影響，屬優先轉換對象。
5. 高價值資產 (High-Value Assets)	數發部、MAS	涉及資產價值較高，如交易金額或延伸的賠償或損失風險較高者。
6. 高頻交易或大量通訊 (High Transaction Frequency)	MAS	涉及即時性或高頻交易的系統（如清算、撮合），風險暴露時窗口期短，應高優先導入。
7. 對外連結與供應鏈依賴 (Third-Party Interconnectivity)	MAS、數發部	依賴第三方 API、供應鏈整合系統，因供應鏈弱點帶來的風險需同步控管並優先規劃。
8. 行為風險性 (Behavioral Risk)	MAS	涉及高風險行為（如:法人,人身道德風險）的應用，將使用行為列為導入優先評估因素。

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

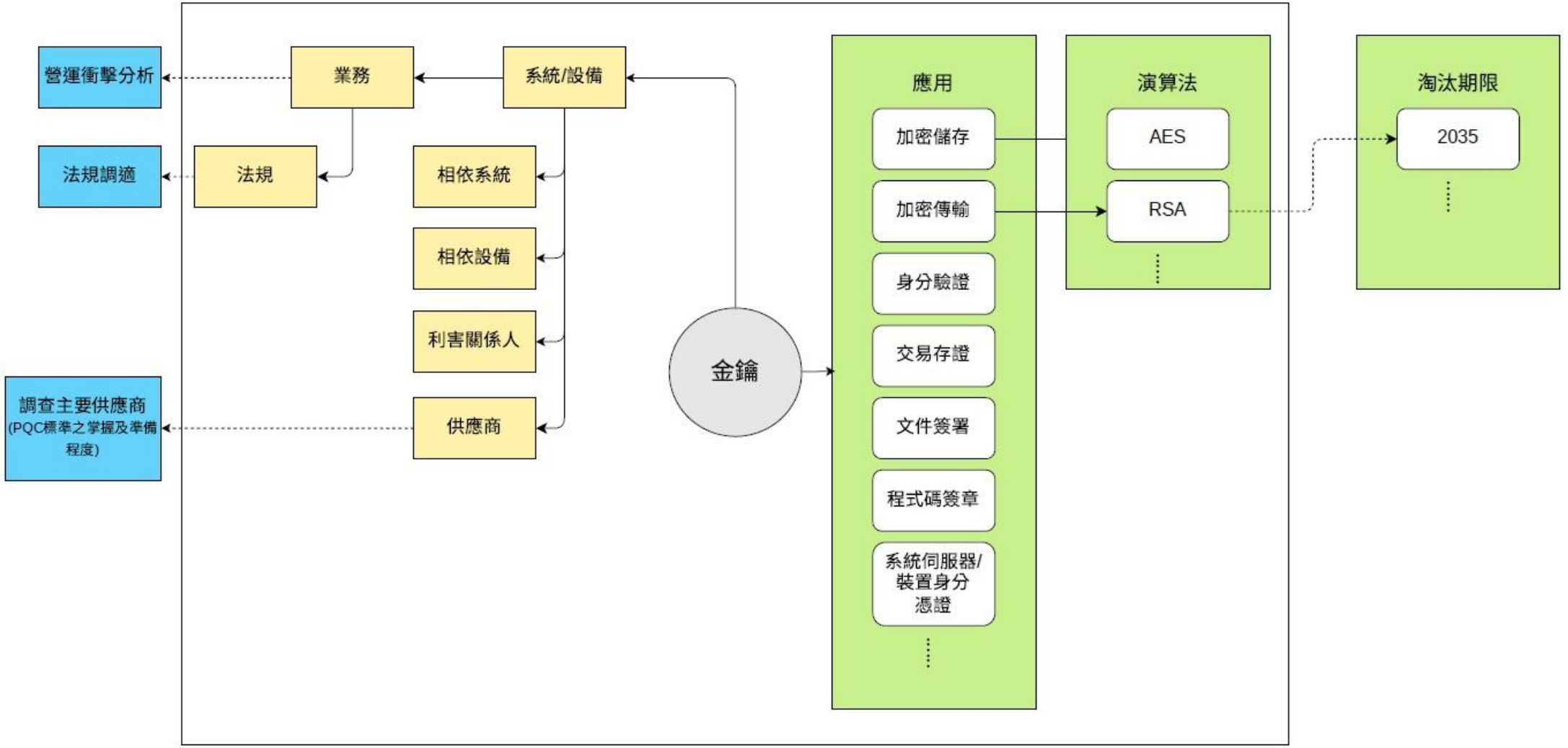
由密碼資產重要性切入→按資產特性

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

由金鑰/憑證關連性切入→密碼技術盤點關鍵項目



資料出處:金管會PQC先導計畫

關鍵場景因應

產品/服務名稱	受影響的單位及範圍	預計因應處理措施
金融 FXML	銀行公會,銀行,客戶(使用FXML 憑證載具)	建議公會規範應立即調整(支援 PQC 及 HSM規格)
金融函證區塊鏈	銀行,會計師,上市櫃公司,財金公司	建議開始盤點並規劃遷移時程
JCIC 信用查詢閘道	證交所,JCIC	與證交所，JCIC 討論規劃中
金融資訊交換平台	證交所,財金公司,銀行,會計機構	目前系統並不支援加密敏捷性，需討論如何更換加密/簽章模組及載具(尚未啟動)
網站安全（TLS 憑證）	全金融業對客戶網頁、API 接口採 TLS 加密之伺服器	• 關注 CA/Browser Forum 進度 • 詢問通訊設備供應商
電子保單	使用電子保單服務的保險公司	• 保單加密支援 AES 256 bits • 通訊閘道升級 (https/ftps)
股票下單安控系統及客戶憑證	證券商交易系統與客戶端電子下單應用（含自然人與法人）	• 已完成 PQC 憑證 POC • 建請提升至SHA 2 (因應過渡準備)
金融 FAST ID（快速身分識別）	提供跨行跨平台身分識別的銀行、財金金融 Fast ID 驗證轉接中心、行動金融應用業者	• 關注 FIDO 組織進度 • 配合金管會及財金公司表定時程辦理

密碼技術初步盤點表 (參考金管會PQC先導計畫草案內容，進行中)

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	

通訊加密/憑證的盤點表 (共用基礎建設)

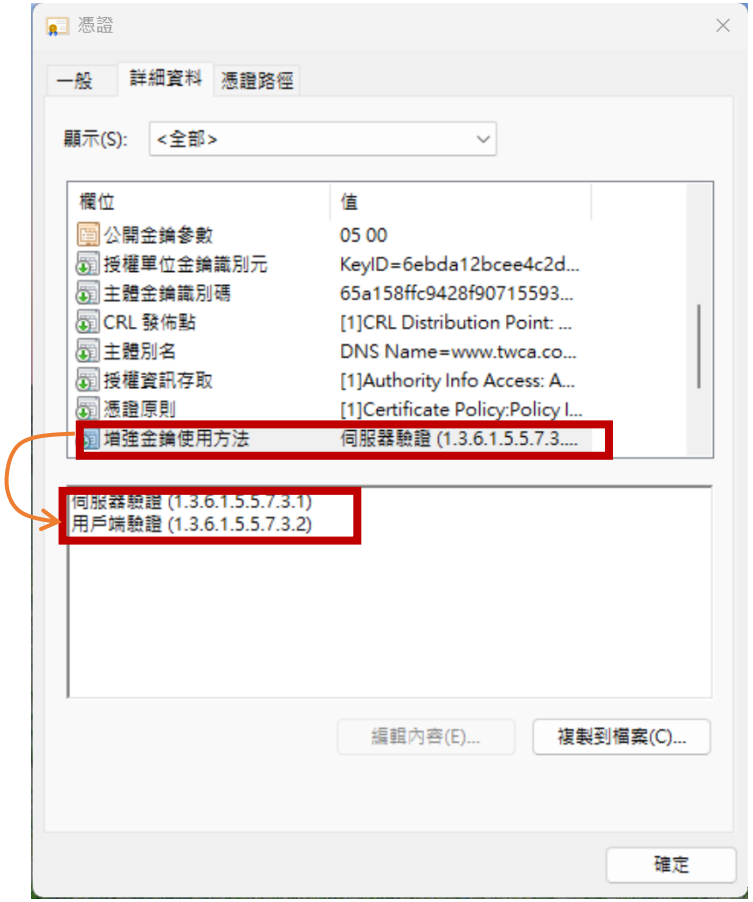
TWCA 整理

	類別	設備	部署位置	連接對象及本身角色(S/C)	通訊協定	TLS 版本(及是否支援 PQC?)	供應商	管理單位	備註
	TLS通訊加密	啟用TLS的設備(以傳輸層為主)	如:DMZ,內網	實際採用TLS交握的對象,並標示本身為Server 或 Client	如:HTTPS, FTPS,VPN, IPSec	• 目前支援最高版本是否支援TLS, 1.3 • PQC加密套件(如:X25519MLKEM768)			
範例	TLS通訊加密	Imperva WAF GW	DMZ	參加單位(Server)	HTTPS	• 目前使用TLS1.2 • 不支援TLS1.3(待韌體升級) • 不支援PQC加密套件(待韌體升級)	中菲	監控處	
	TLS通訊加密	EnterpriseDT ComplateFTP	DMZ	參加單位(Server)	FTPS	• 目前使用TLS1.2 • 支援TLS1.3(待軟體升級) • 不支援PQC加密套件(未提供)	EnterpriseDT	管理處	

	類別	憑證識別名稱(CN或SAN)	簽發單位	產製金鑰工具	供應商	憑證佈署設備/主機	供應商	管理單位	備註
	TLS站台憑證	填寫**主要名稱(CN)**及**主旨別名(SAN)**	CA名稱	填寫金鑰產製工具名稱與版本		憑證佈署設備或主機			
範例	TLS站台憑證	• www.twca.com.tw • download.twca.com.tw • ssl.twca.com.tw • www.taica.com.tw • twca.com.tw	TWCA	openssl 3.5	openssl	• Imperva WAF GW • Apache HTTP Server 2.4.65 • IIS 10.0	• 中菲 • Apache • Microsoft	管理處	

TLS/SSL 憑證自2026年6月起,不得再提供 ClientAuth(用戶端驗證) 功能

如何知道憑證是否具有「用戶端驗證」功能？



新憑證鏈 (2025.07.01 起，不再有用戶端驗證功能)	**原憑證鏈** (2026.06.15 之後，規定無法再提供)
第1層：TWCA Global Root CA	第1層：TWCA Global Root CA
第2層：TWCA CYBER Root CA	第2層：TWCA Secure SSL Certificate Authority
第3層：TWCA SSL Certificate Authority	(EV 憑證為：TWCA Global EVSSL Certificate Authority)
(EV 憑證為：TWCA EVSSL Certificate Authority)	第3層：server cert (用戶之站台憑證)
第4層：server cert (用戶之站台憑證)	

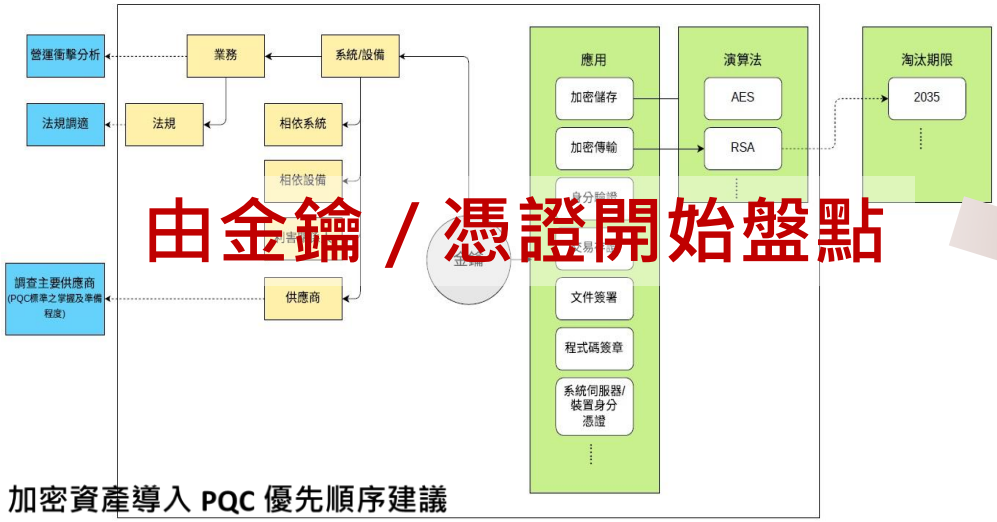
[註1] https://googlechrome.github.io/chromerootprogram/

若用戶仍有用戶端驗證需求，可另外向 TWCA 申請 AP憑證。

TLS 遷移策略建議

階段	時間範疇	主要行動	關鍵責任方
前置作業	預計2025	1. IETF X.509 納入 PQC (2025 Oct公告) 2. NIST FIPS 140-3 Level 3 PQC 認證標準 3. CA Browser Forum 相關標準 4. 網站盤點(和 TLS CA 合作) 5. 內部 Client Auth 盤點(因應 Chrome 要求 TLS 憑證不能做為 AP to AP使用,客戶可改申請 AP 憑證) 6. 瀏覽器最低版本建議升級至 Modern 7. 通訊設備盤點是否支援 TLS	1. IETF 2. NIST 3. CA 4. 金融機構和 CA 5. 金融機構 6. 金融機構 7. 金融機構和設備供應商
準備期	2025-2027	• 逐步要求瀏覽器最低版本採用 PQC • 逐步採購或升級支援 PQC 的設備 (如:通訊設備)	
過渡期	2028-2030	• CA 試營運 PQC TLS憑證 • 通訊設備全面升級	CA 通訊設備
完成期	2030 以後	• TLS 網站憑證完全採用 PQC	全生態系統

結論1：評估密碼資產導入 PQC (參考金管會 PQC 先導計畫)



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	使用者與客戶端互動	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（5年以上）保密性需求	高（P1）	電子報單
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）	

由業務特性開始盤點

可再分別討論 P0 ,P1 ,P2 ,P3 的具體時程

密碼技術初步盤點表 (參考金管會PQC先導計畫草案內容，進行中)

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	

2025/12/2 Copyright of TWCA 30

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）

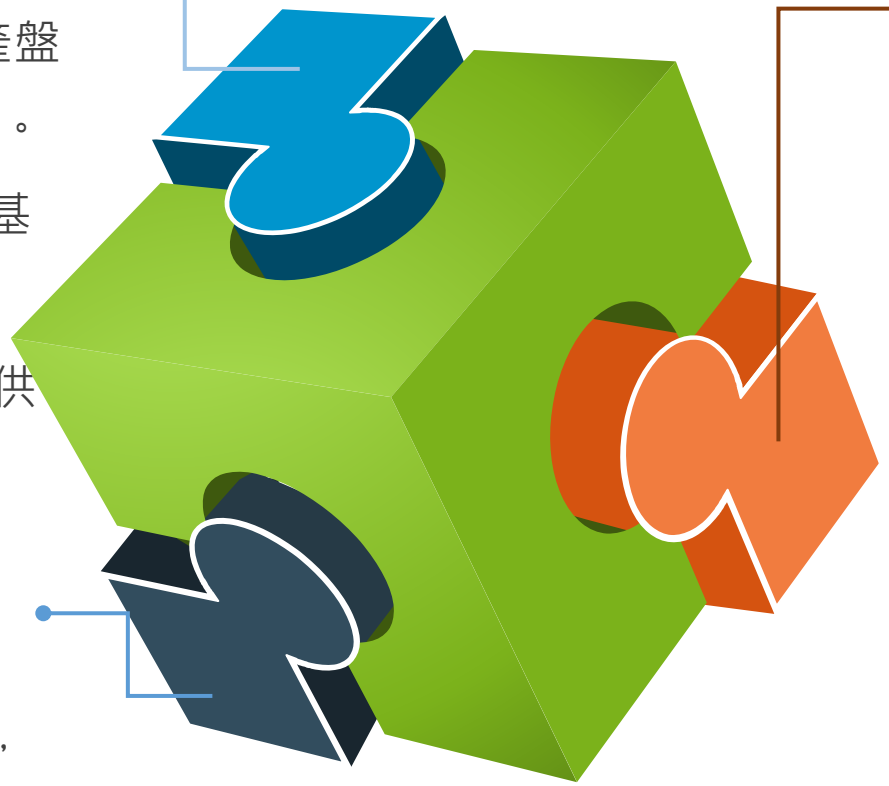
結論與呼籲

立即 盤點密碼資產與業務場景

- 參考金管會先導計畫密碼資產盤點表進行盤點 (金鑰 or 場域)。
- 通訊加密/TLS憑證/CA盤點 (基礎建設)。
- 使用工具 (如:CBOM) 或詢問供應商。

密切追蹤國際標準，分階段導入 PQC

- 密切注意國際標準與法規調整，逐步啟動導入 PQC 準備工作。



與供應商協作，確保系統具備加密敏捷性

- 請供應商提供遷移評估問題清單，以了解 PQC Ready 程度。
- 確認現有系統達到基本要求 (TLS 1.3, AES 256 bits, RSA 2048 bits, SHA 2)
- 新一代系統應具備**加密敏捷性** (減少應用系統與加解密演算法的相依性)。