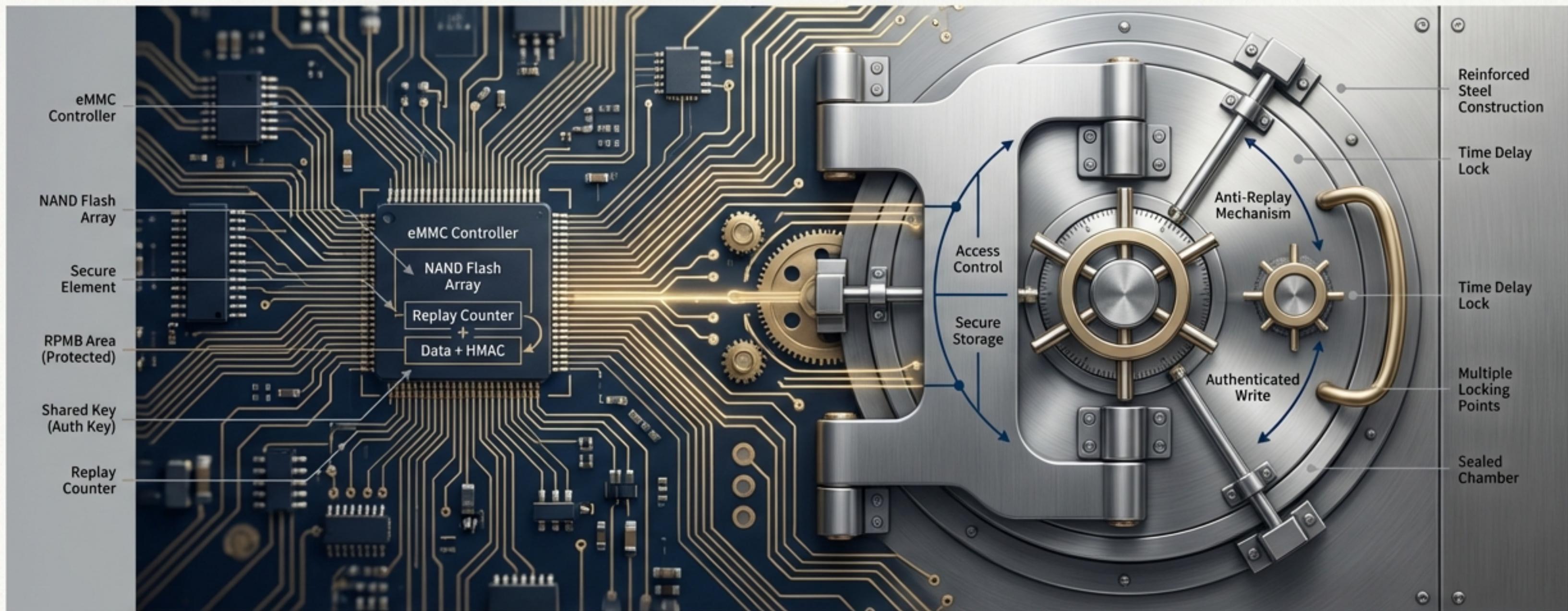


# eMMC RPMB：打造無法撼動的數位保險箱

## Replay Protected Memory Block 技術深度解析



# 潛伏的威脅：為何傳統儲存機制並不足夠？

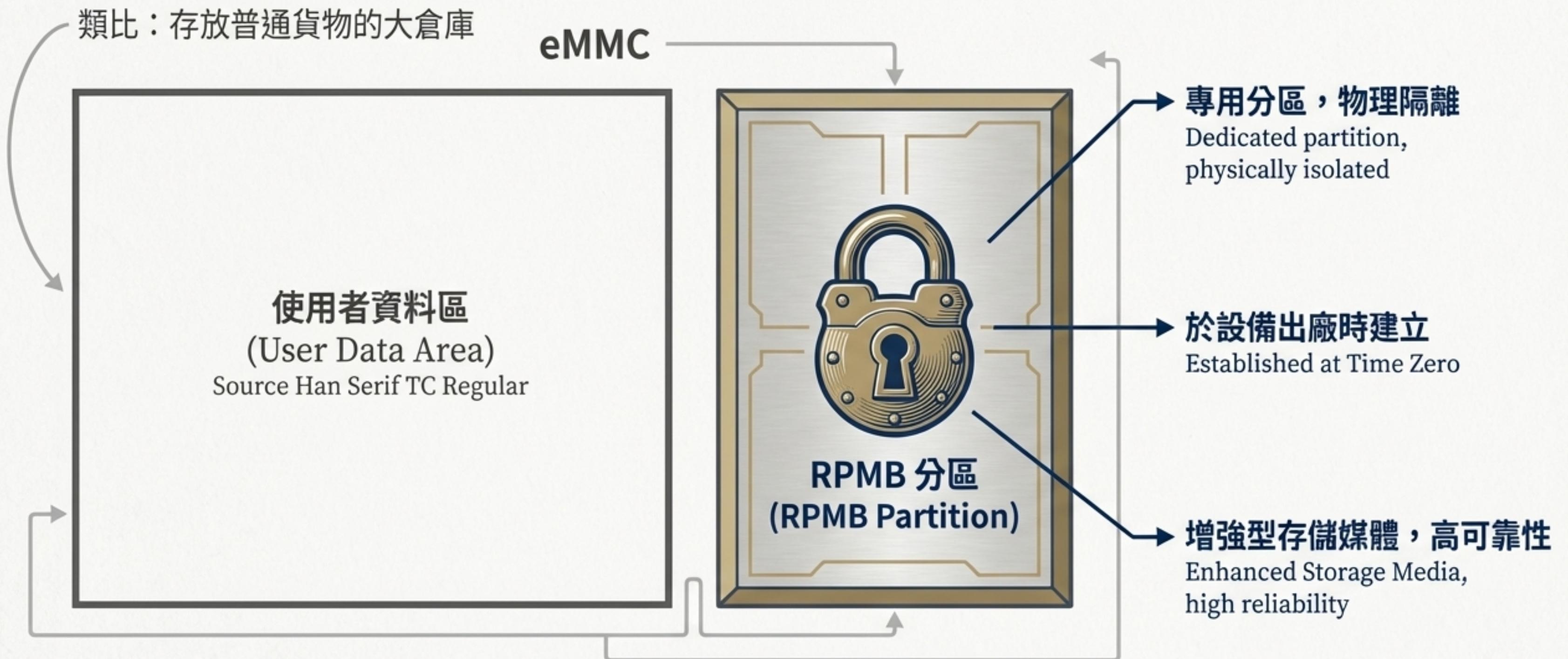
介紹「重放攻擊（Replay Attack）」的核心概念。攻擊者只需錄製一個有效的指令（例如「支付\$10」），然後不斷「重播」它，就能造成巨大危害。這是一種欺騙，而非破解。



類比說明：這就像竊賊影印了一張你過去的有效提款單，然後試圖拿著影本重複到銀行提款。如果銀行沒有核對機制，就會輕易受騙。

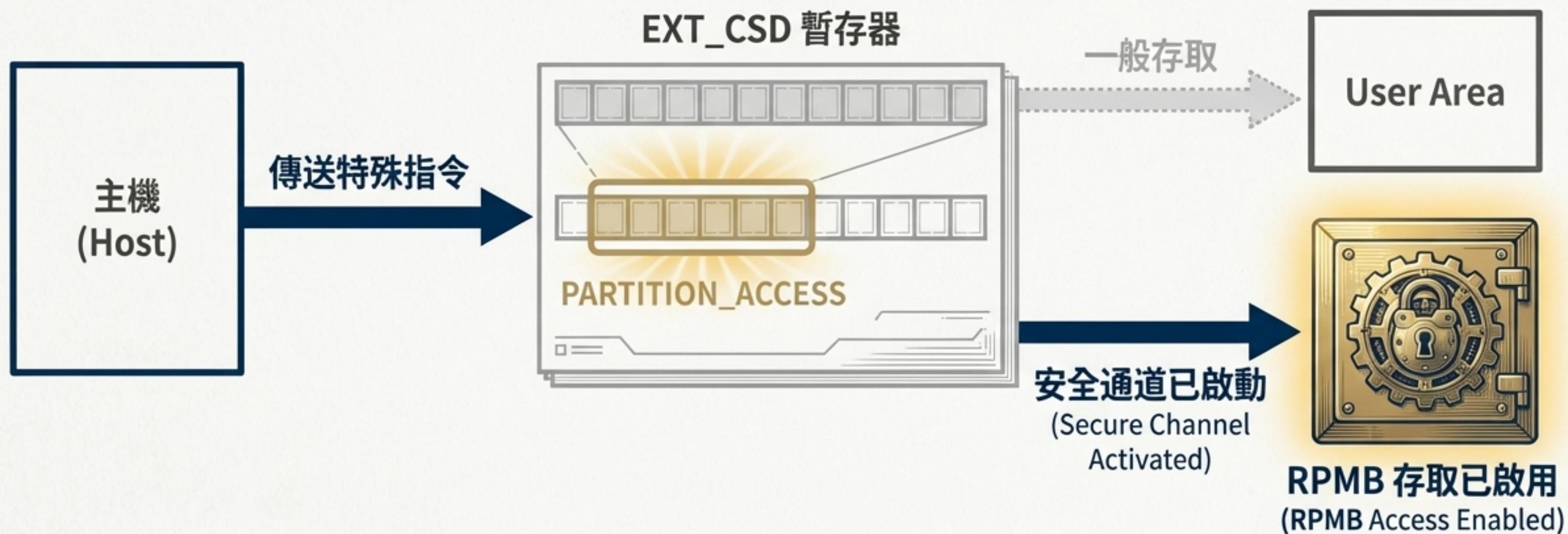


# 解決方案：一個具備記憶與驗證能力的專屬保險箱



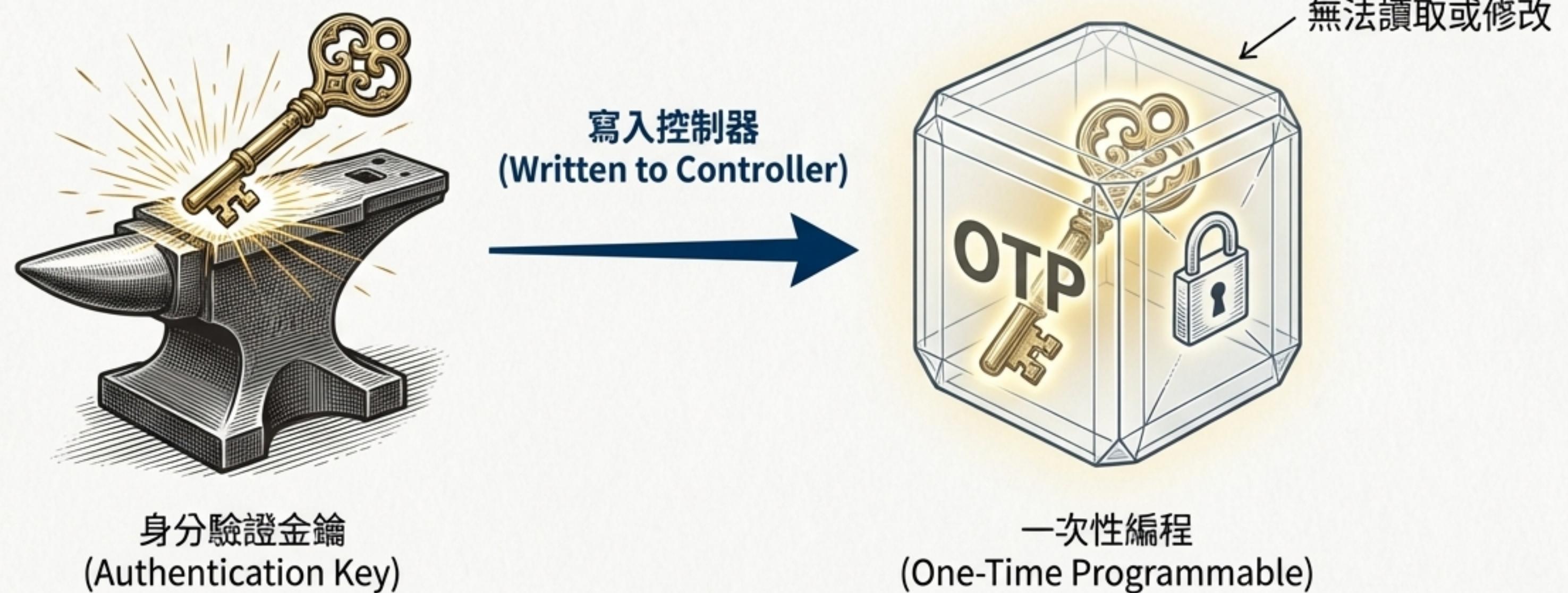
# 啟動安全通道：切換至 RPMB 存取模式

要存取這個保險箱，你不能走常規通道。你必須使用一個特殊的指令序列，向「銀行總管」（eMMC 控制器）表明你的意圖。



# 信任之錨：鑄造一把獨一無二且無法複製的鑰匙

我們現在要鑄造一枚獨特的魔法印章（金鑰）。你（主機）和銀行總管（控制器）會各持有一枚完全相同的複製品。一旦鑄造完成，這枚印章就會被永久封存，永遠無法被再次讀取、複製或修改。



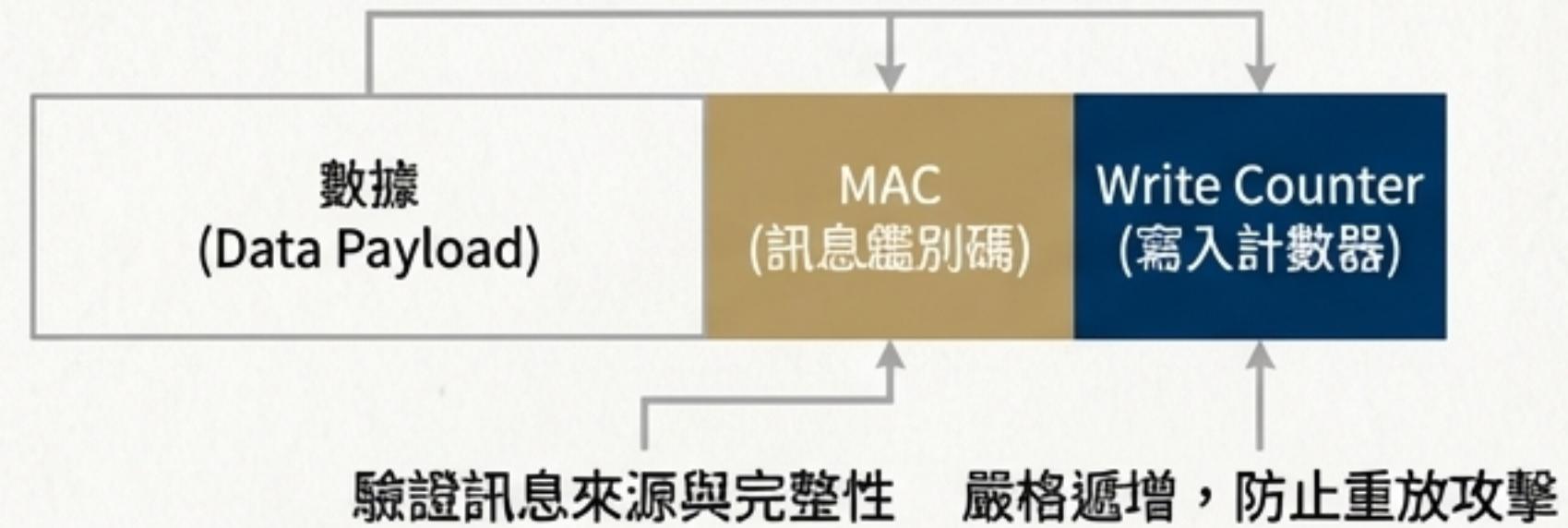
# 安全握手協議：每一筆交易都需簽名與編號

## 類比：簽名與帳本



每一份請求單，都必須蓋上印章並寫上連續的流水號，缺一不可。

## 技術實現：驗證與計數

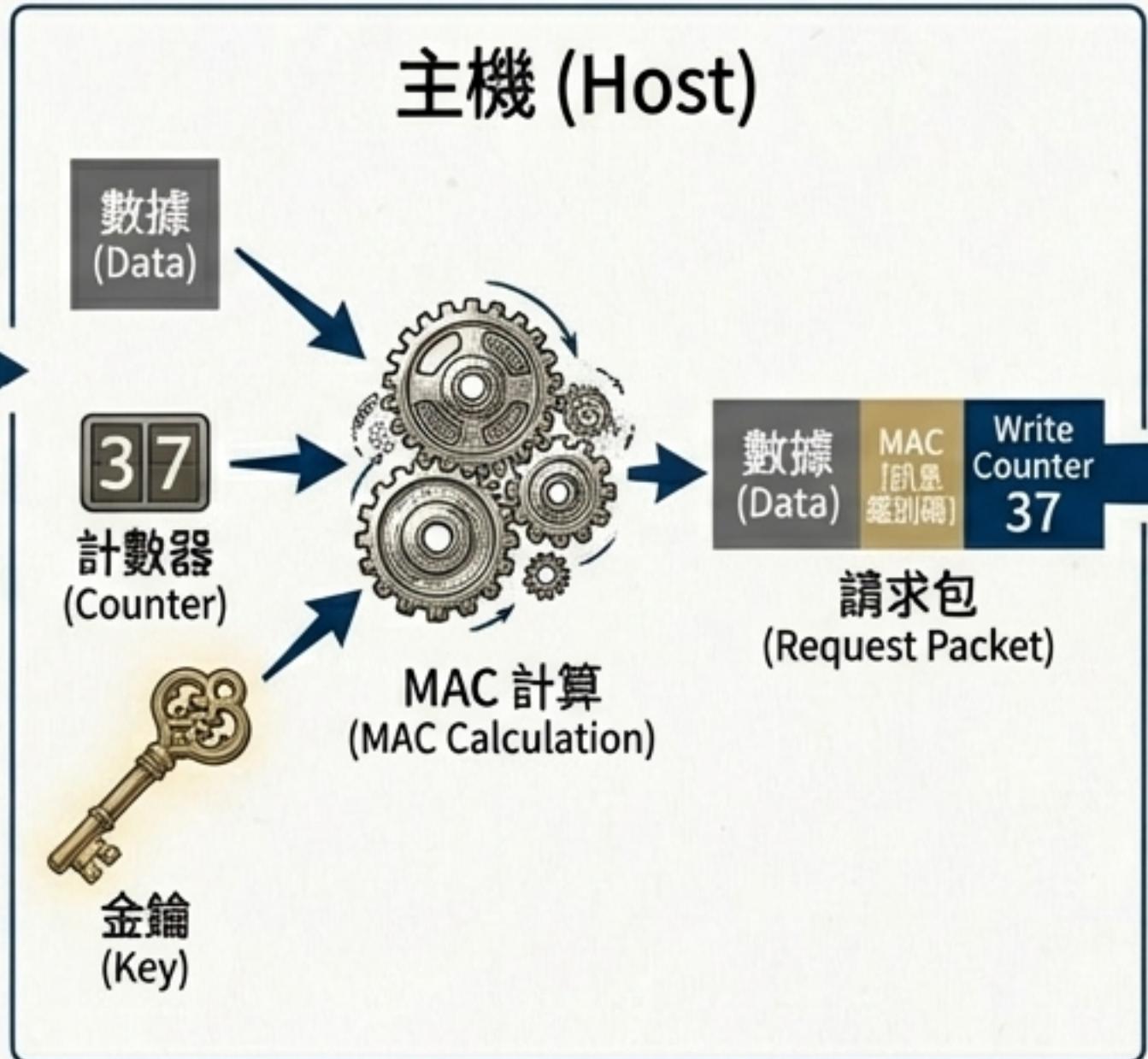


# 安全存入：將數據放入保險箱的嚴謹流程

3步



3步 2: 產生請求包



3步 3: 設備驗證與寫入

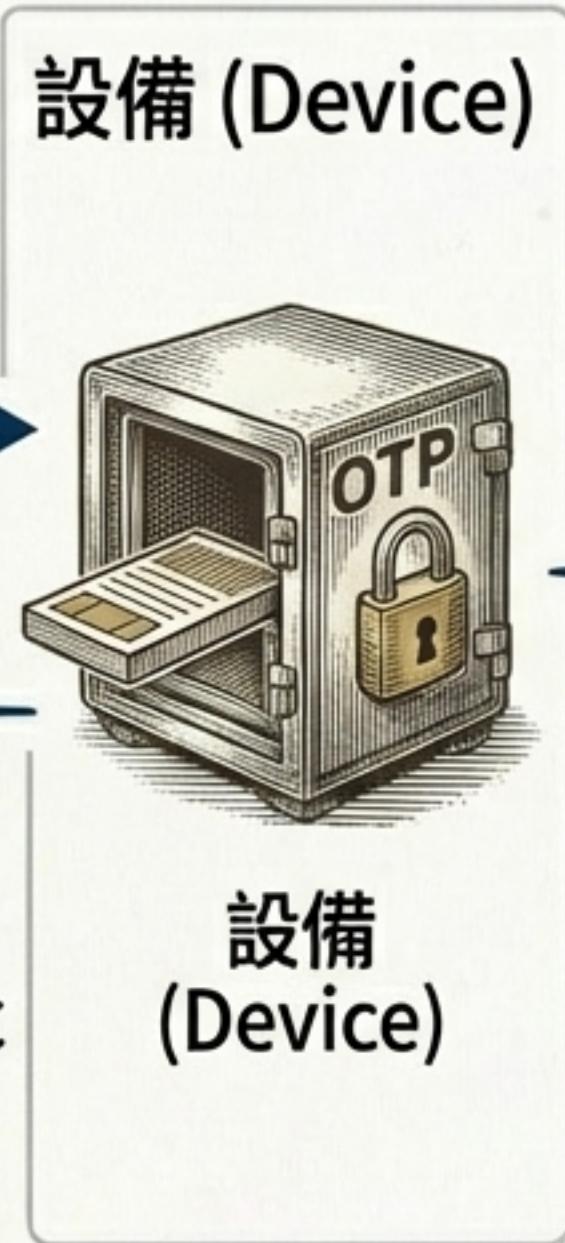


# 認證讀取：如何驗證從保險箱取出的數據

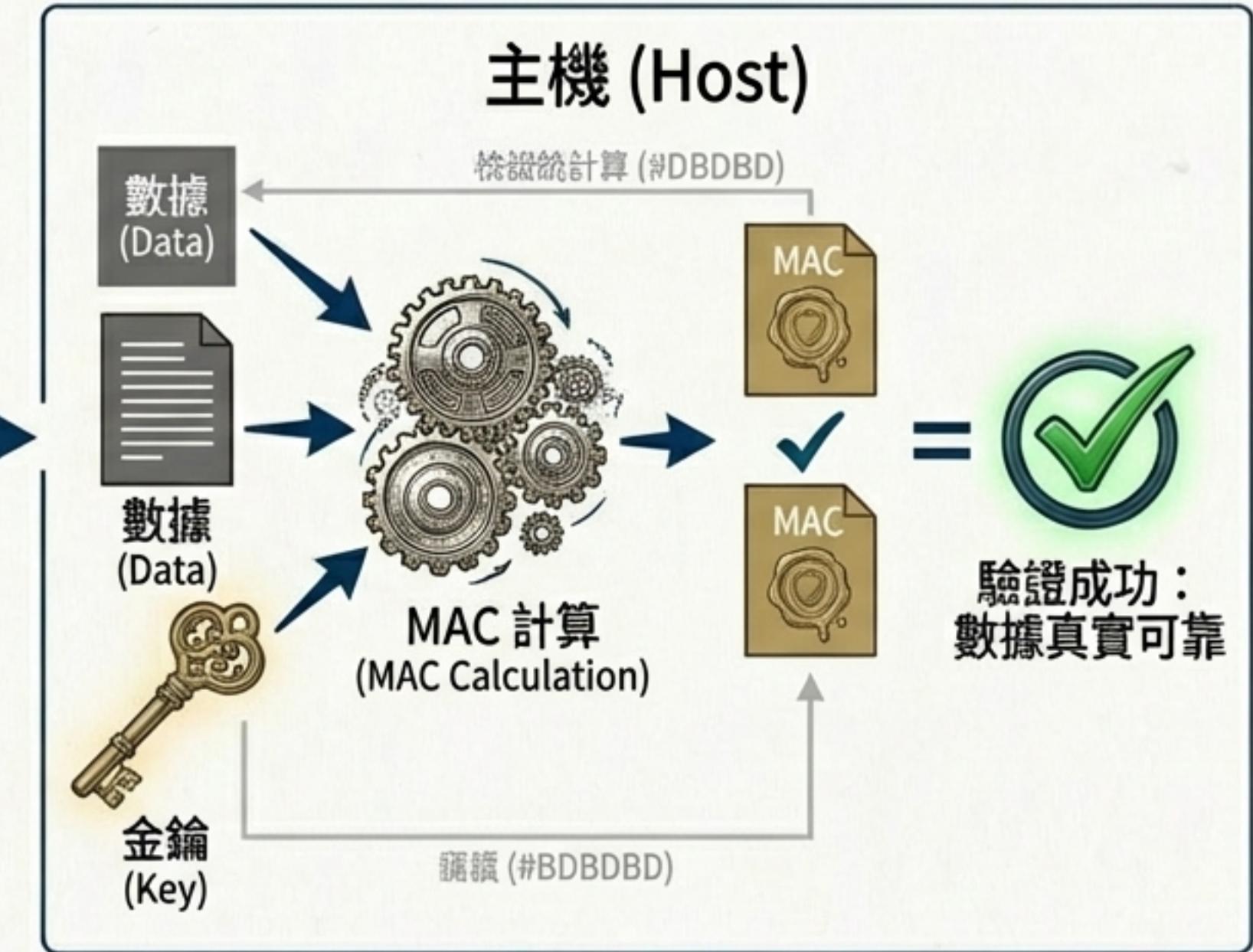
3步



3步



3步



# 意外防護機制：即使在斷電瞬間也能確保數據完整

**類比：**保險箱的門被設計成原子操作，要麼完全打開，要麼完全關閉，絕不會卡在中間，確保地震（斷電）時內容物安然無恙。



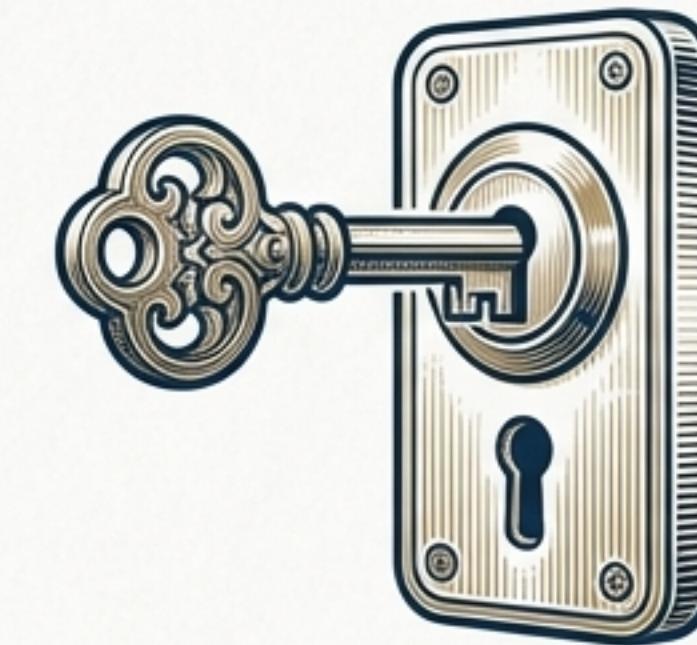
**技術細節：**RPMB 利用 eMMC 的「可靠寫入 (Reliable Write)」特性，確保寫入操作是原子性的，防止因意外斷電導致的數據損毀。

# 保險箱裡的珍寶：RPMB 的關鍵應用場景



## 安全啟動 (Secure Boot)

儲存啟動程式碼 (bootloader) 的雜湊值 (hash)。系統啟動時會進行比對，確保啟動鏈未被惡意篡改。



## 數位版權管理 (DRM)

安全地儲存內容解密金鑰。這些金鑰永遠不會暴露在非安全區域。



## 防回滾保護 (Anti-rollback)

儲存韌體的版本號。防止攻擊者透過安裝有已知漏洞的舊版韌體來攻擊設備。

其他敏感數據：如支付憑證、指紋資料、加密金鑰等重要資訊。

# 安全守則：有效管理您的數位保險箱



## 金鑰配置 (Key Provisioning)

身份驗證金鑰的寫入是極度敏感的操作。它必須在物理安全的環境中完成，例如在工廠的生產線上，以防止金鑰在出廠前洩漏。



## 計數器管理 (Counter Management)

雖然設備會驗證計數器，但主機端有責任正確地管理和使用計數器。錯誤的管理可能導致合法的寫入請求被拒絕，或產生安全漏洞。主機必須確保計數器的使用是連續且無誤的。

# RPMB 的絕對優勢：晶片中的安全堡壘



## 硬體級隔離 (Hardware Isolation)

專用的物理分區，與使用者數據完全隔離，提供了天然的保護屏障。



## 不可逆的信任根 (Irreversible Trust)

一次性編程 (OTP) 的金鑰，一旦設定便無法讀取或修改，建立了永久且可靠的trust基礎。

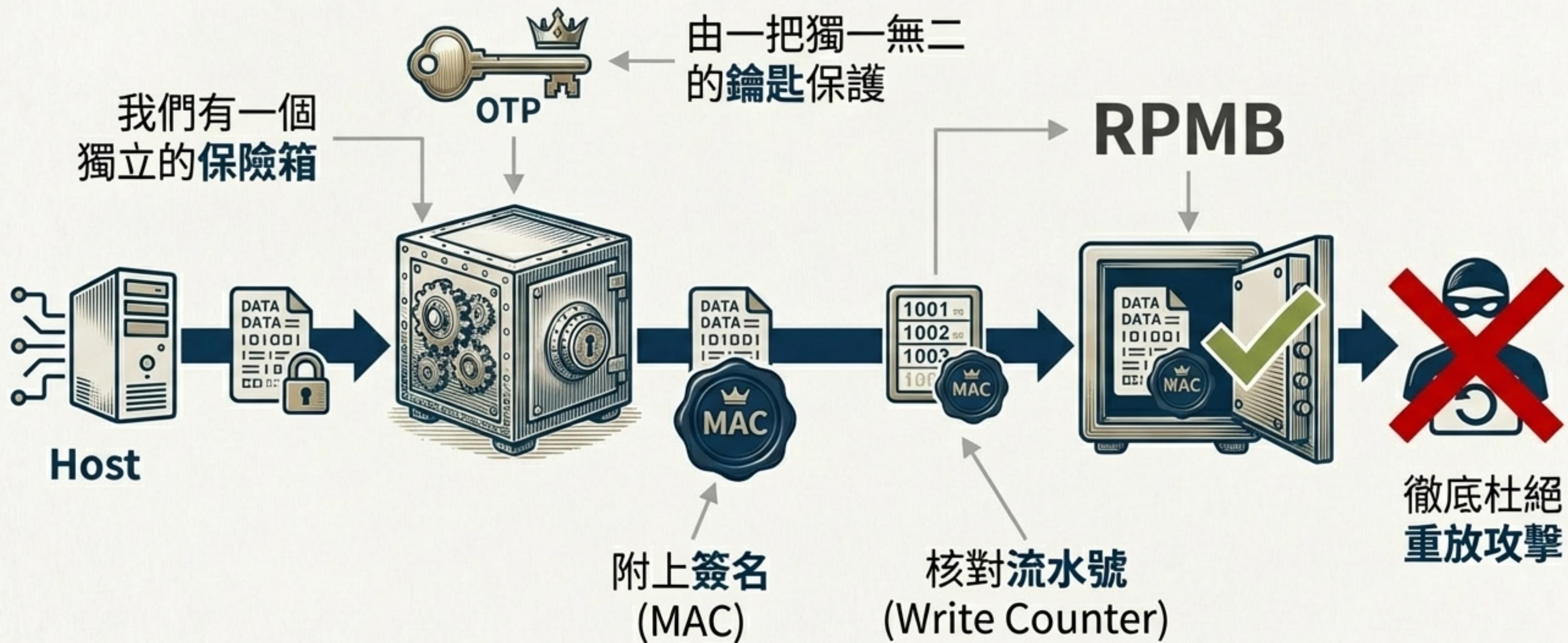


## 認證與完整性 (Authenticated Integrity)

強大的 MAC 與計數器機制，確保了每一筆數據的來源可靠性、內容完整性，並能有效抵禦重放攻擊。



# 數位保險箱運作全覽



# 謝謝

## Q&A

---