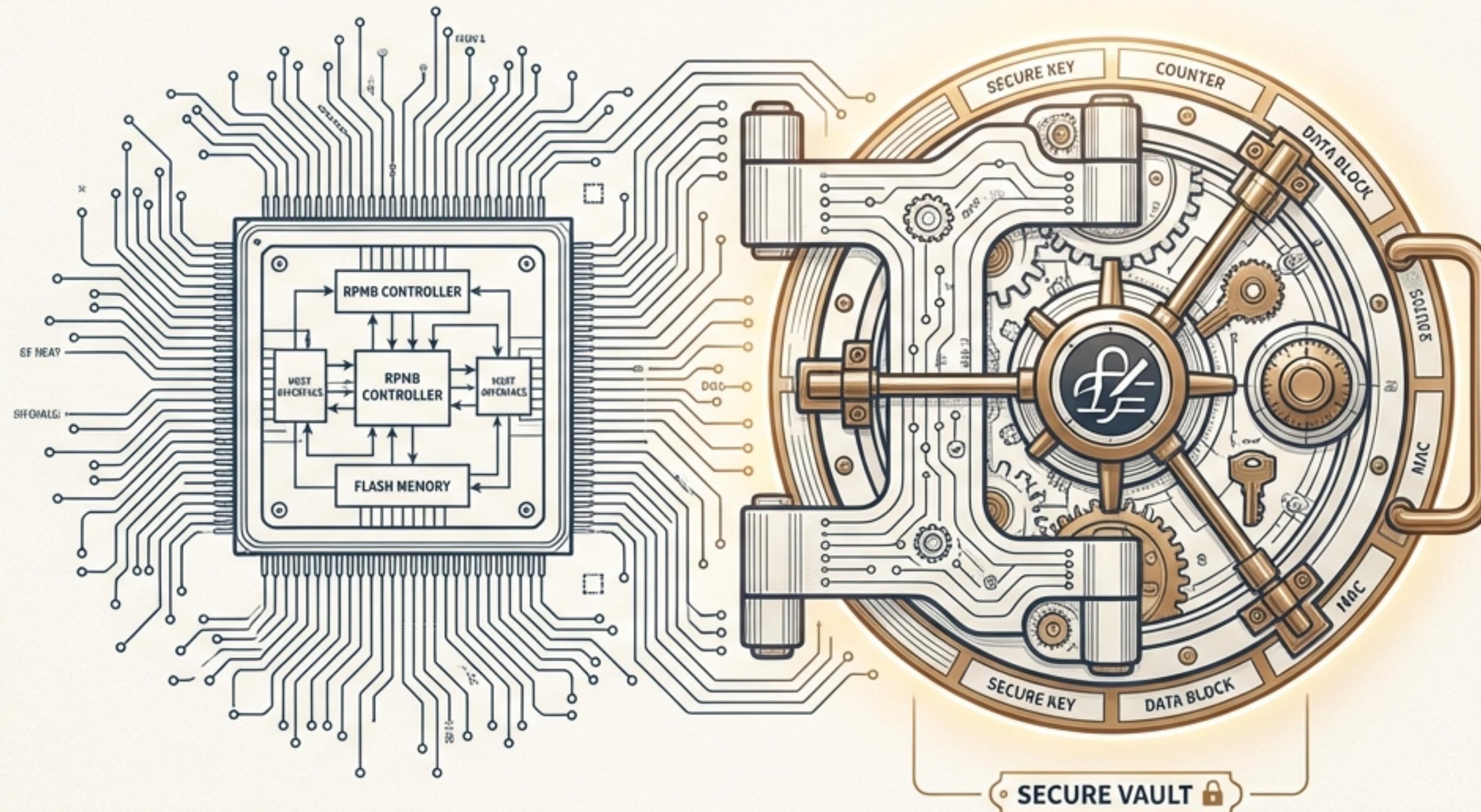


eMMC RPMB：精通你的數位金庫

一份基於「動態印章保險箱」模型的實務指南



數位世界中的信任危機

當數據可以被輕易複製與竄改時，我們如何保護最關鍵的秘密？



關鍵挑戰



數據竄改：未經授權的修改，破壞系統完整性。



重放攻擊：攔截並重送舊的、合法的指令，造成非預期的操作。

這些威脅對於以下應用是致命的：



安全金鑰



支付資訊



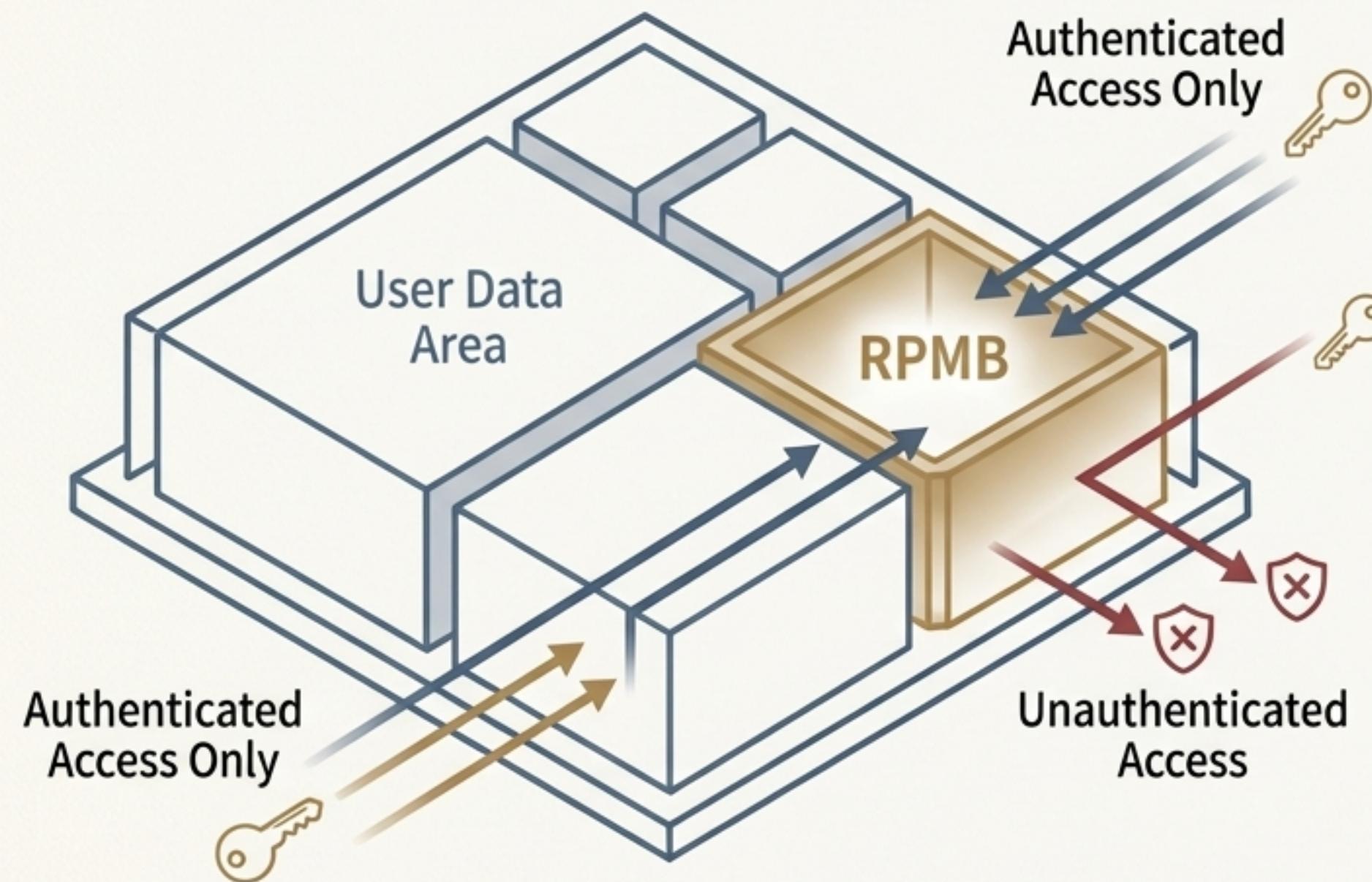
防回滾版本號



生物特徵數據

解決方案：一座內建於 eMMC 的數位金庫

RPMB (Replay Protected Memory Block)：一個提供以「認證過」且「防重放攻擊」方式存取數據的專用系統區域。



The Metaphor Explained



保險箱 (The Safe Deposit Box)
RPMB 是一個獨立、受硬體保護的儲存空間。



動態印章 (The Dynamic Stamp)
一種基於共享秘密金鑰的加密簽名 (MAC)，確保指令來源於您。



流水號簽收單 (The Serialized Receipt)
一個只能增加、無法倒退的計數器 (Write Counter)，確保每條指令都是全新的。

金庫的藍圖：物理與邏輯架構

獨立分區 (Independent Partition)

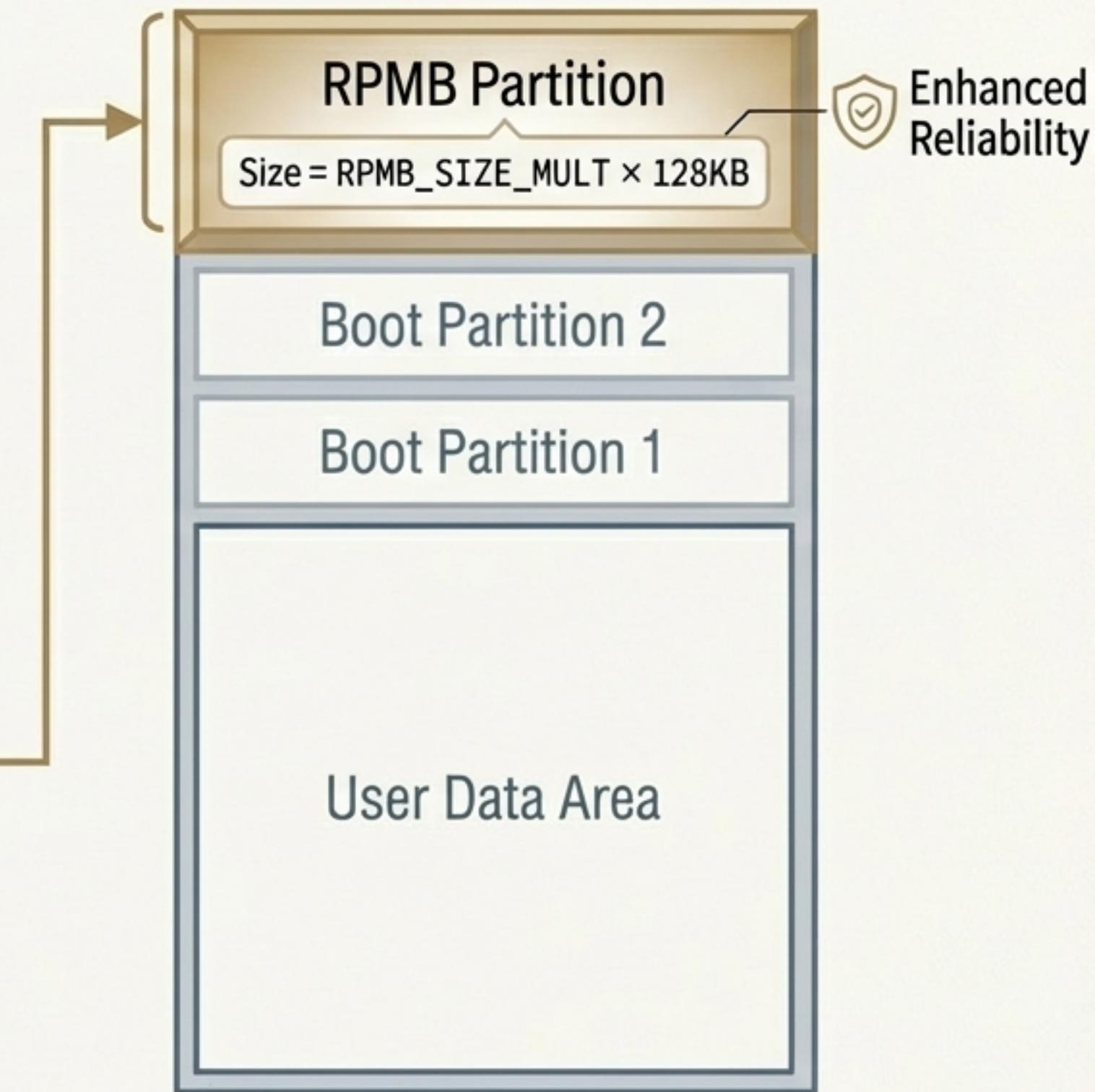
- 在設備出廠時 (Time Zero) 即已存在，獨立於用戶數據區 (User Data Area)。
- 視覺化為 eMMC 記憶體空間的一個獨立區塊。

容量規模 (Capacity)

- 大小由 EXT_CSD 中的 RPMB_SIZE_MULT 欄位決定。
- 容量 = RPMB_SIZE_MULT x 128KB。

媒體特性 (Media Characteristics)

- 預設配置為「增強型存儲媒體」(Enhanced Storage Media)。
- 這意味著更高的數據可靠性與耐久度，專為關鍵數據設計。



鑄造金庫鑰匙：獨一無二的身份驗證金鑰

金鑰是主機 (Host) 與 RPMB 之間的信任根源。

核心特性 (Core Properties)

- 一次性編程 (One-Time Programmable, OTP)：
 - 金鑰儲存在專用暫存器中。
 - 一經寫入，便永遠無法被讀取或再次修改。
- 絶對安全 (Absolute Security)：
 - 金鑰的寫入過程必須在極端安全的環境中完成，例如 OEM 的安全生產線。
 - 一旦設定，金鑰本身不會在任何通訊中傳輸，只用於內部計算「動態印章」(MAC)。



警告：此操作不可逆！

儀式一：打開通往金庫的秘密通道

存取 RPMB 前，必須先切換 eMMC 的作用分區。

CMD6 (SWITCH)

1. 目標

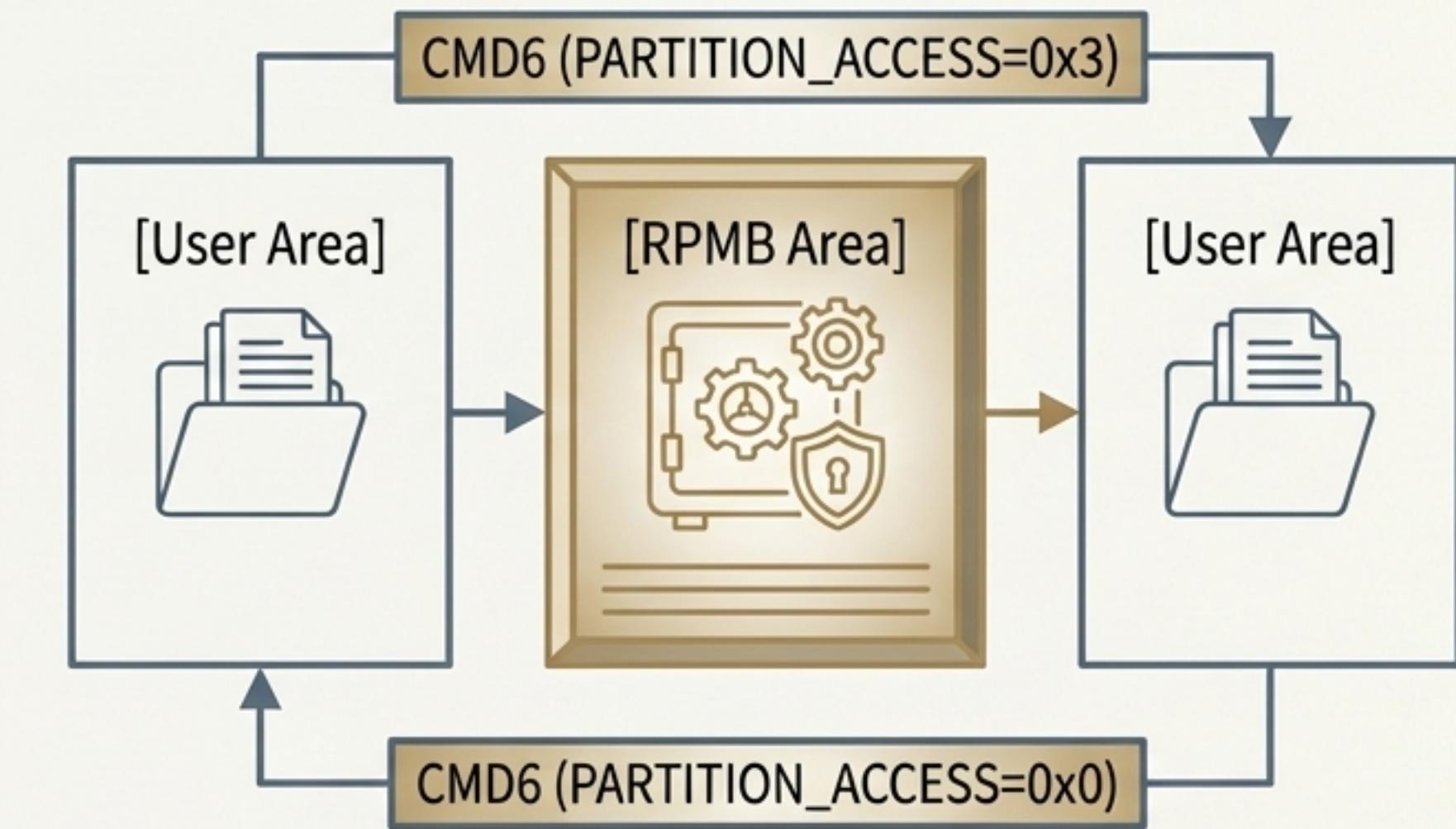
修改 EXT_CSD 暫存器的 [179] 位元組。

2. 參數

將 PARTITION_ACCESS 欄位的值設為 0x3。

3. 結果

之後的所有讀寫指令都將指向 RPMB 分區。



存取完畢後，必須再次使用 CMD6 將分區切換回原本的設定。

儀式二：準備溝通的咒語



CMD23

(SET_BLOCK_COUNT)

預告傳輸規模 (Announcing the Transaction Size)

在任何讀寫操作前，必須先用此指令定義要傳輸的數據塊數量。

關鍵細節 (CRITICAL DETAIL):

寫入數據時，參數的第 31 位元 (Reliable Write Request) 必須設為 1。This ensures the atomicity of the write operation.



CMD25

(WRITE_MULTIPLE_BLOCK)

發送請求

(Sending a Request)

所有送往 RPMB 的「請求」都使用此指令，無論是讀取還是寫入。



CMD18

(READ_MULTIPLE_BLOCK)

接收響應

(Receiving a Response)

用於從 RPMB 獲取操作結果或讀取出的數據。

解構秘密訊息：512 位元組數據幀

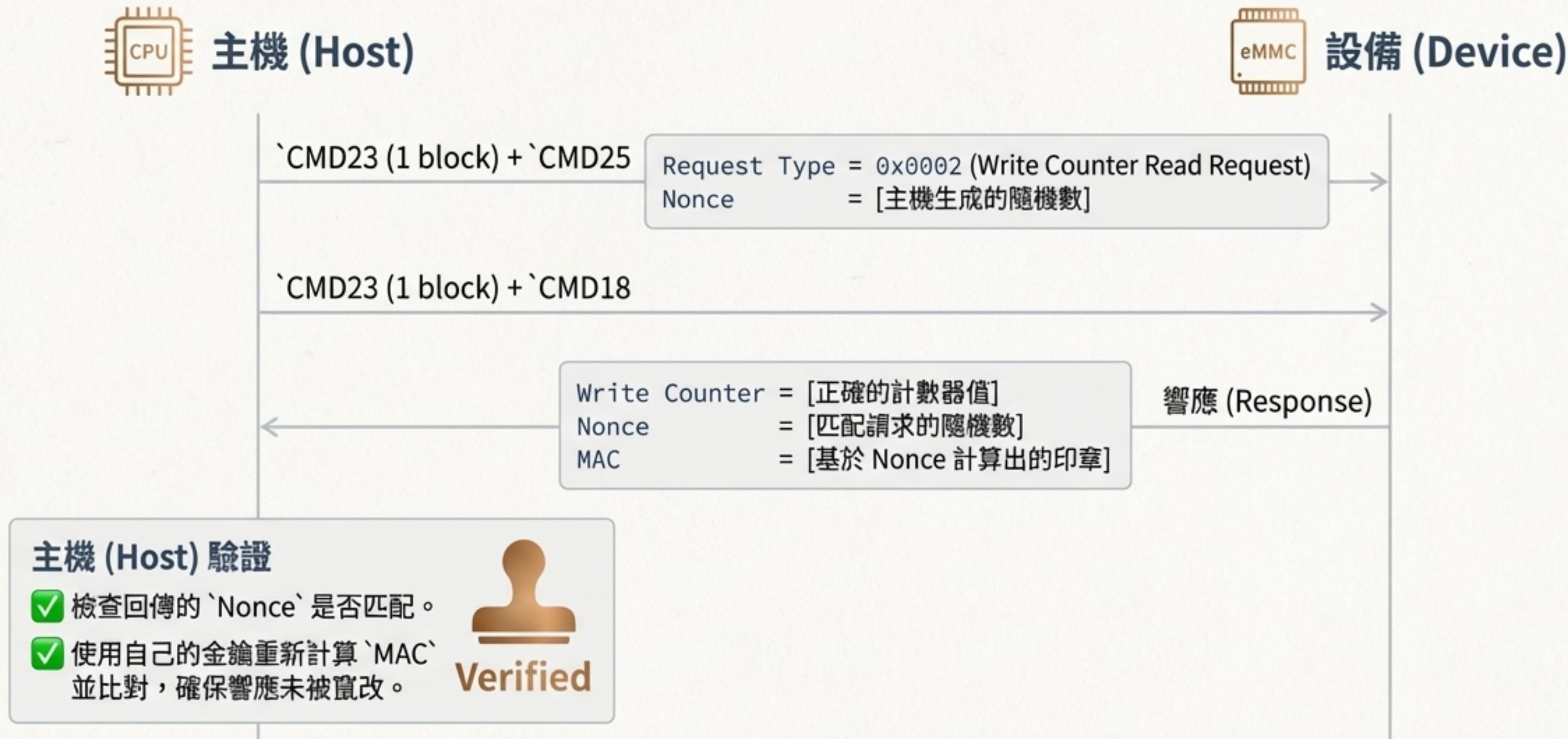


Request/Response Type (2 Bytes)

角色：申請表格類型 (The Request Form Type)
說明：定義操作類型，例如金鑰寫入 (0x0001)、計數器讀取 (0x0002)、數據寫入 (0x0003)。

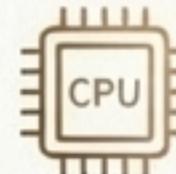
實戰流程一：查詢簽收單的最新流水號

目的：在寫入任何數據前，必須先獲取當前計數器的值，以防重放攻擊。



實戰流程二：安全存入數據

目的：將數據寫入 RPMB，同時確保操作的認證性與原子性。



主機 (Host)

Step 1: 主機 (Host) 準備



獲取最新的‘Write Counter’
(如上一頁流程)。



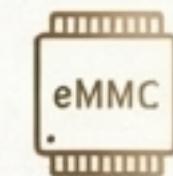
準備 256 字節的‘Data’。



將‘Write Counter’值加一。



計算包含‘Data’和新‘Write Counter’的‘MAC’(動態印章)。



設備 (Device)

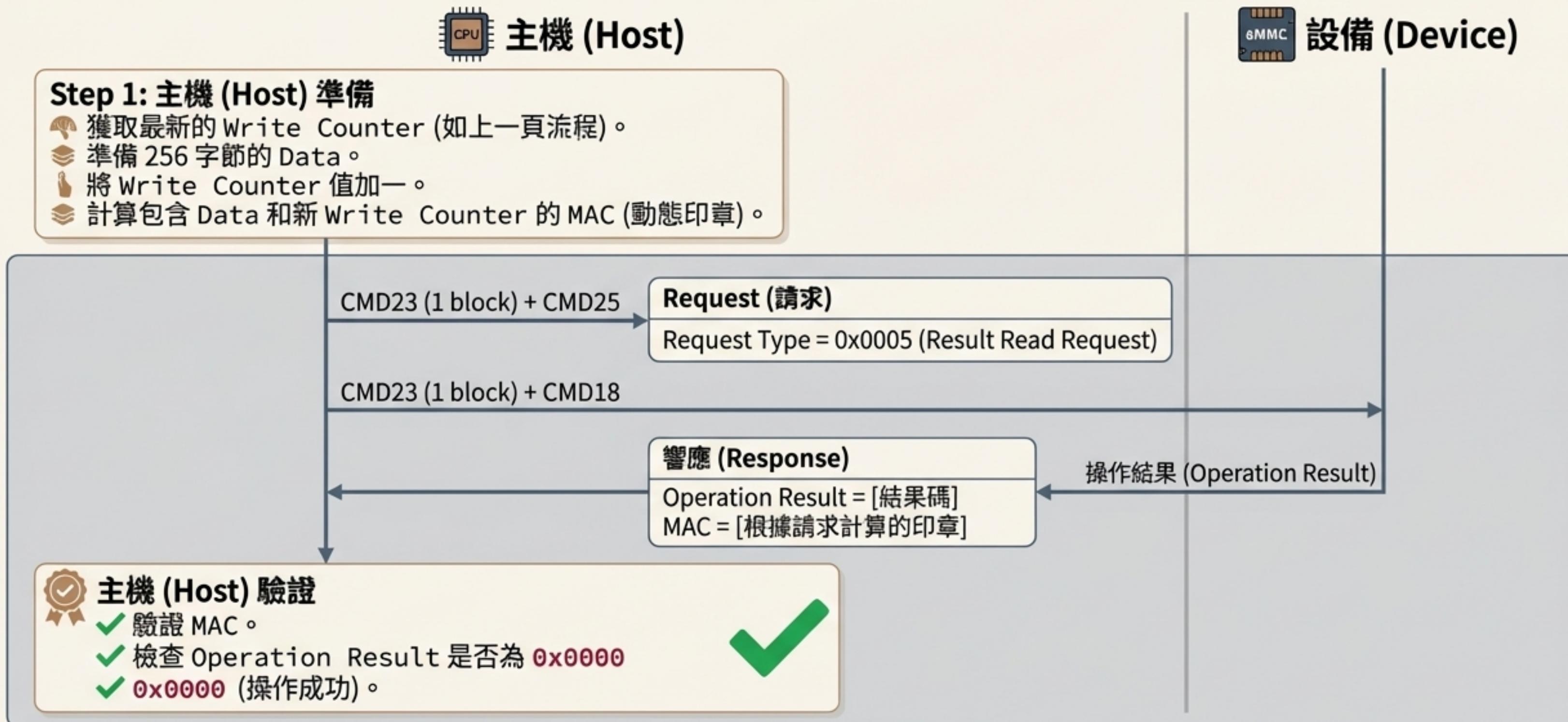
‘CMD23 (Reliable Write=1) + ‘CMD25

Request (請求)

Request Type	= 0x0003 (Authenticated Data Write)
Write Counter	= [最新值 + 1]
Data	= [你的數據]
MAC	= [計算出的印章]

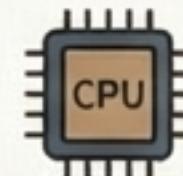
實戰流程二（續）：確認數據已被簽收

目的：寫入操作後，必須主動查詢結果以確認成功。

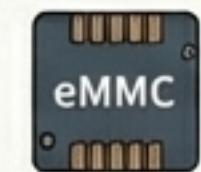


實戰流程三：安全讀取數據

目的：從 RPMB 讀取數據，並驗證其來源真實、內容未被竄改。



主機 (Host)



設備 (Device)

Step 1:

CMD23 (1 block) * + CMD25

Request Type = 0x0004 (Authenticated Data Read)
Address = [欲讀取的數據地址]
Nonce = [主機生成的隨機數]

Step 2:

CMD23 (n blocks) + CMD18

數據響應 (Data Response)
Data = [請求的數據]
MAC = [從 Data 和 Nonce 計算出的印章]



主機 (Host) 驗證

- ✓ 主機使用收到的 Data 和自己發送的 Nonce 重新計算 MAC。
- ✓ 比對計算出的 MAC 與設備回傳的 MAC 是否一致。



設備回傳的 MAC = 主機計算的 MAC

當儀式出錯：解讀金庫管理員的警報

操作結果在 *Result Read Request* 的響應幀中提供。



0x0000 **OK**

管理員說

「一切順利。」



0x0002 **Authentication Failure**

管理員說

「你的動態印章是偽造的。」

原因

MAC 不匹配，可能金鑰錯誤或計算錯誤。



0x0003 **Counter Failure**

管理員說

「你的流水號簽收單已經過期了。」

原因

主機提供的 Write Counter 不是設備期望的值，疑似重放攻擊。

大師級技巧：為金庫加上永久鎖

Advanced Feature (eMMC 5.1+):

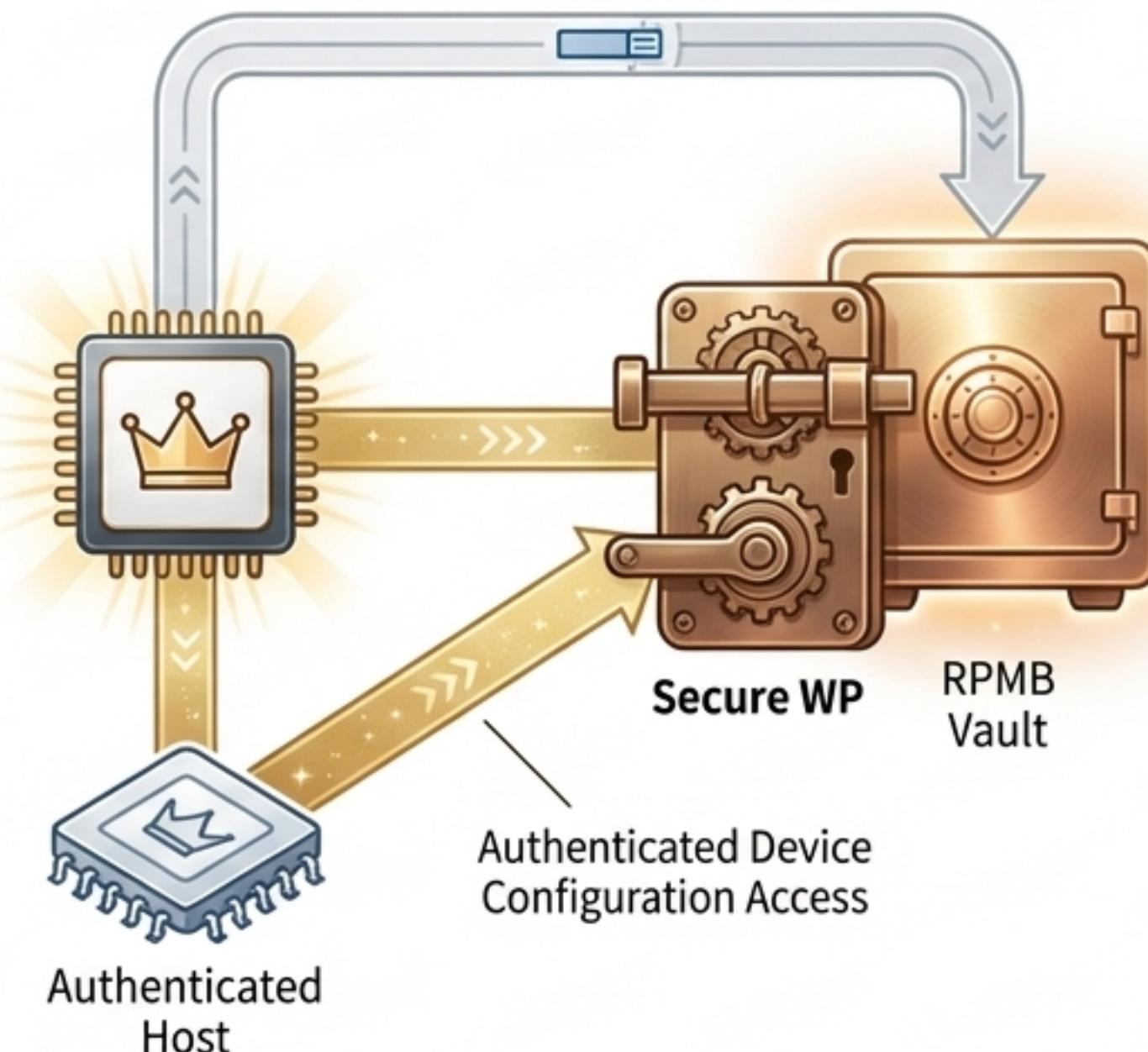
安全寫入保護模式 (Secure Write Protect Mode)

除了 RPMB 的常規讀寫保護外，還可以透過一個經認證的配置區，來設定更強的、基於硬體的寫入保護。

- **Authenticated Device Configuration Area:** 只有通過認證的指令才能修改此區域的設定。
- `SECURE_WP_EN` 位元：使用此位元可以防止任何人（即使是合法的 Host）未經授權就更改寫入保護的狀態。



Analogy：這就像為你的保險箱設定了一個只有你才能啟動或解除的定時鎖。



你，現在是數位金庫的守護者



RPMB不是單純的加密儲存，它是一個完整的、基於硬體的信任系統。



秘密金鑰 (Secret Key) :
信任的根源，永不洩漏。



動態印章 (MAC) :
保證了指令的真實性
(Authenticity)。



流水號簽收單 (Write Counter) :
杜絕了重放攻擊 (Replay Attacks)。

透過精通這些儀式，您能夠在任何 eMMC 系統中建立一個堅不可摧的數據安全堡壘。