

精通 e·MMC 安全性：CMD42 密碼保護機制深度解析



從概念到指令，一份完整的實作與管理指南

數位保險庫的基石：密碼保護功能的核心概念

定義

允許主機透過提供密碼來 **鎖定** 設備，防止未經授權的數據存取。

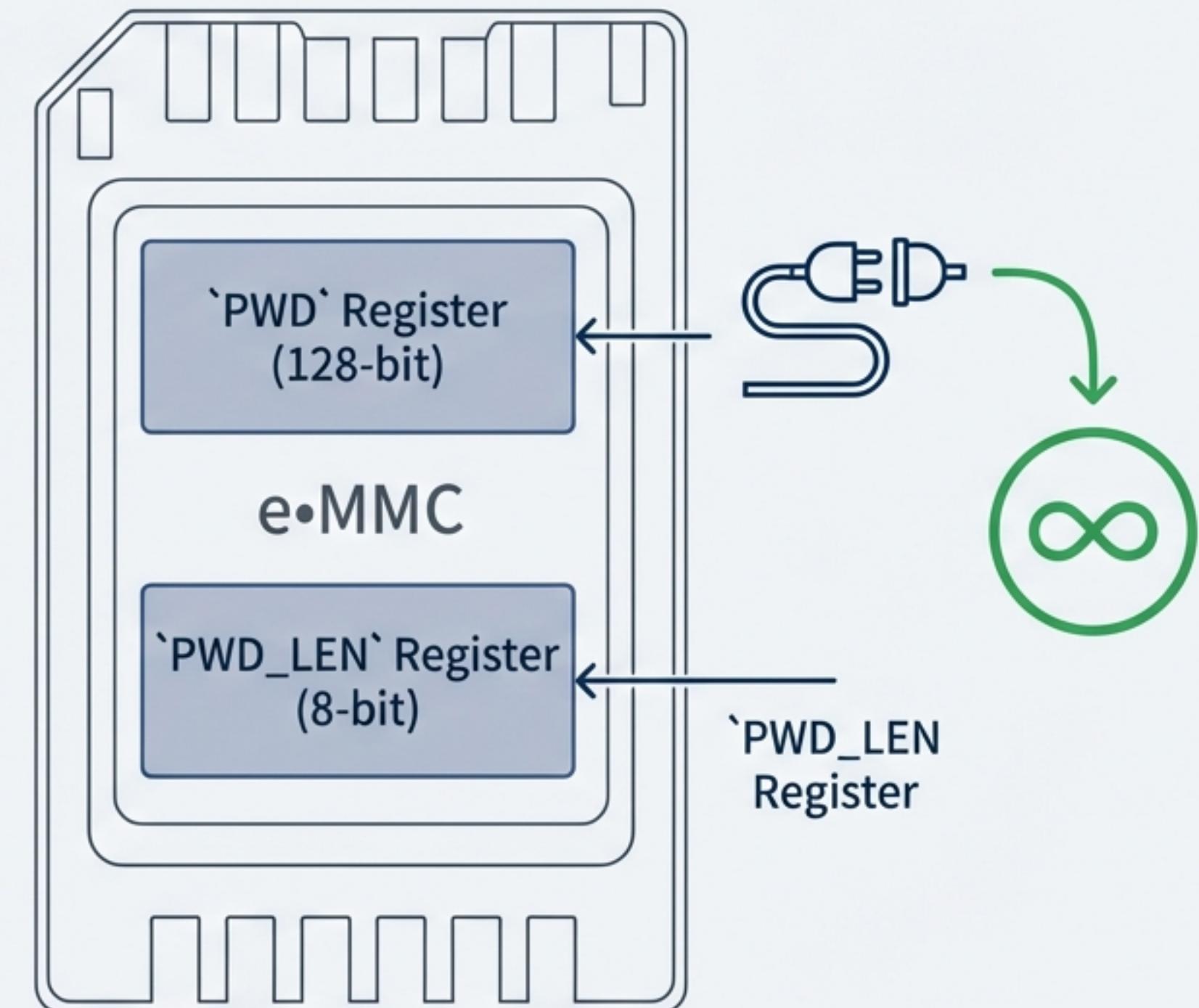
核心暫存器

- PWD (128-bit)：用於儲存密碼的非揮發性暫存器。
- PWD_LEN (8-bit)：用於儲存密碼長度的非揮發性暫存器。



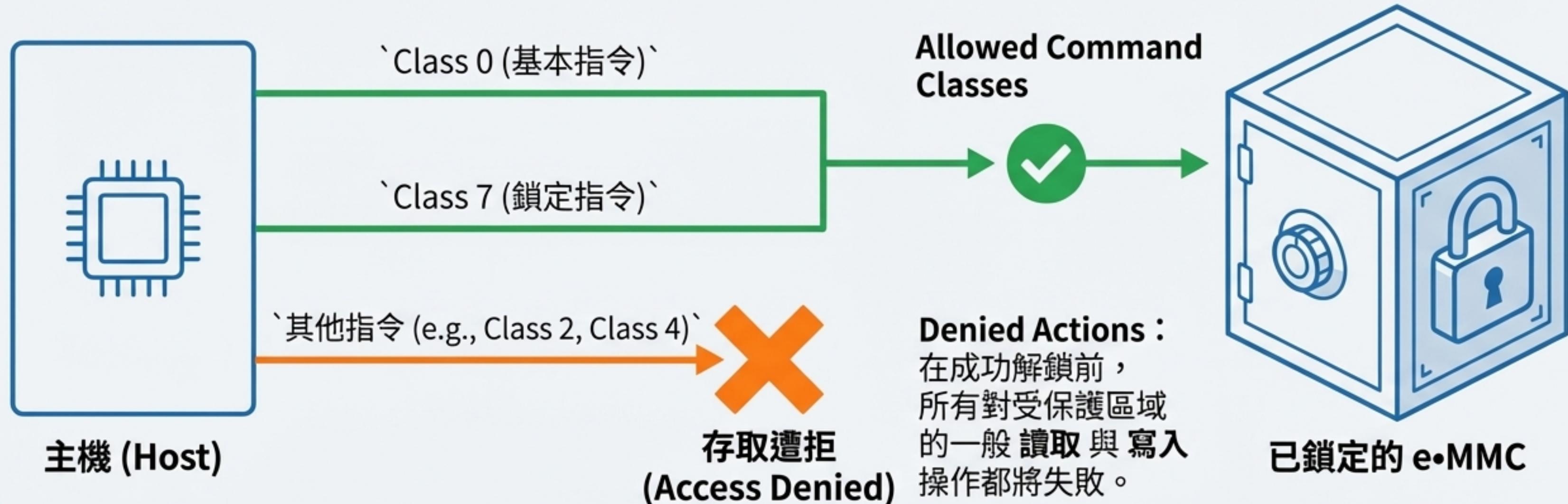
持久性 (Persistence)

密碼與長度資訊儲存在非揮發性記憶體中，即使在設備掉電後也不會消失。

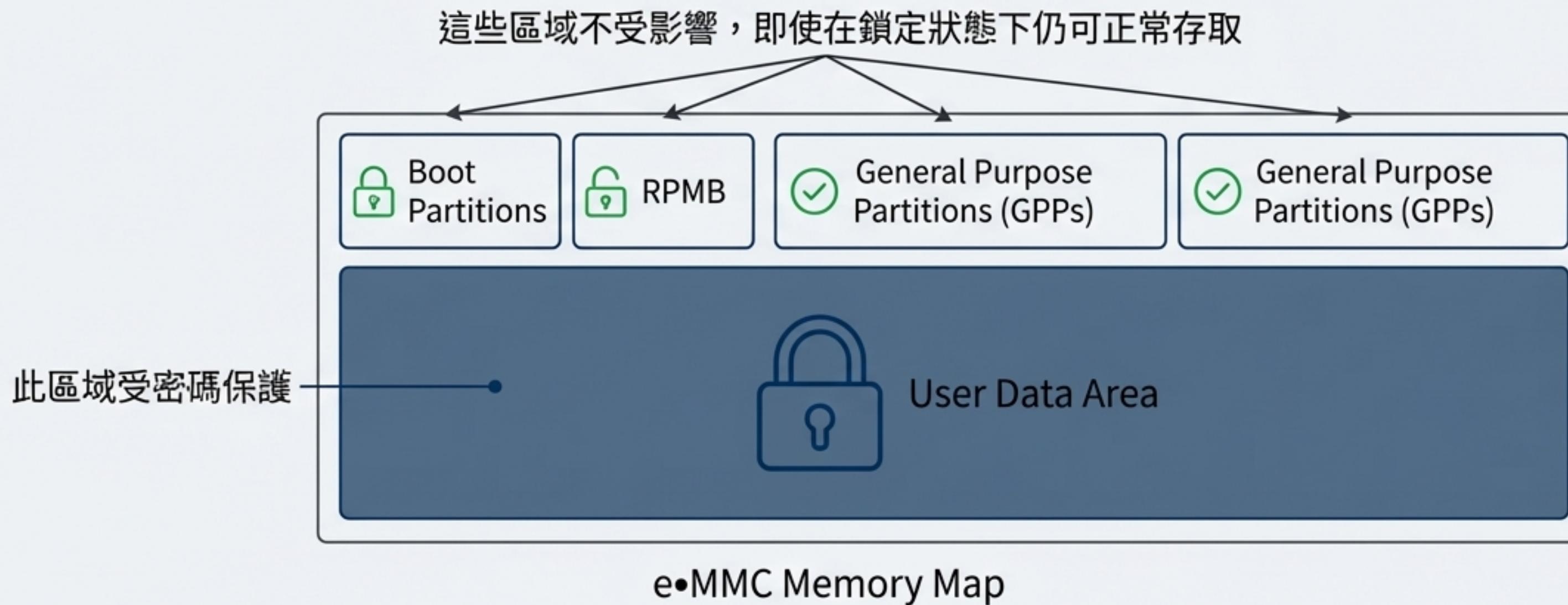


鎖定狀態下的設備行為：有限的指令響應

一旦設備被鎖定，其功能將受到嚴格限制，絕大多數數據存取指令會被拒絕。



劃定界線：密碼鎖定的範圍與限制 (v4.3+)



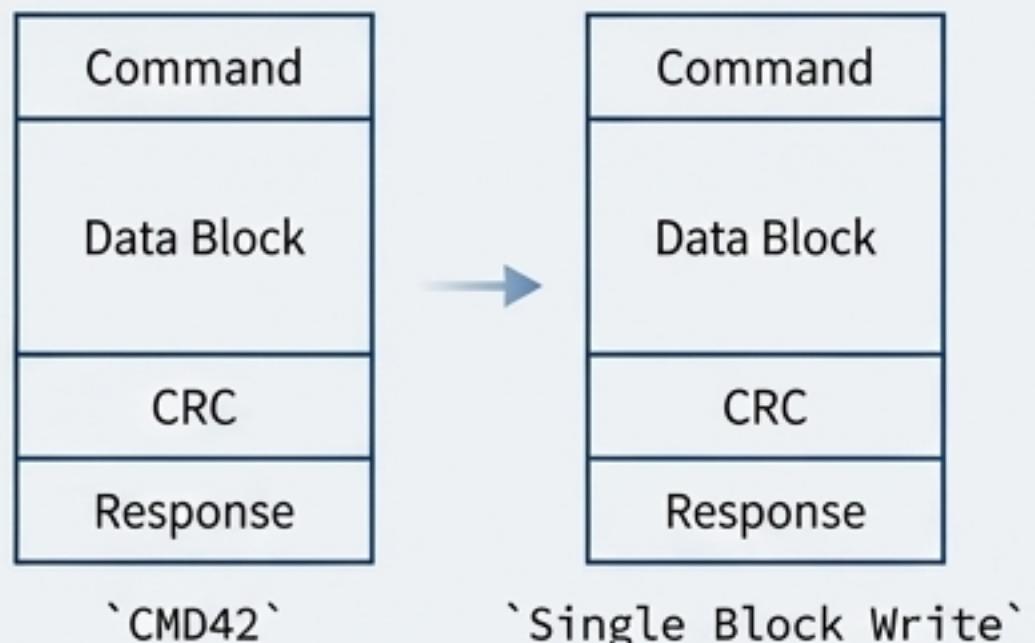
類比：倉庫大門的數位掛鎖

這就像鎖住了倉庫 (User Data Area) 的大門，但獨立的辦公室 (Boot/GPP) 與
保險櫃 (RPMB) 仍然可以透過各自的通道進出。

執行 CMD42 的協議規則

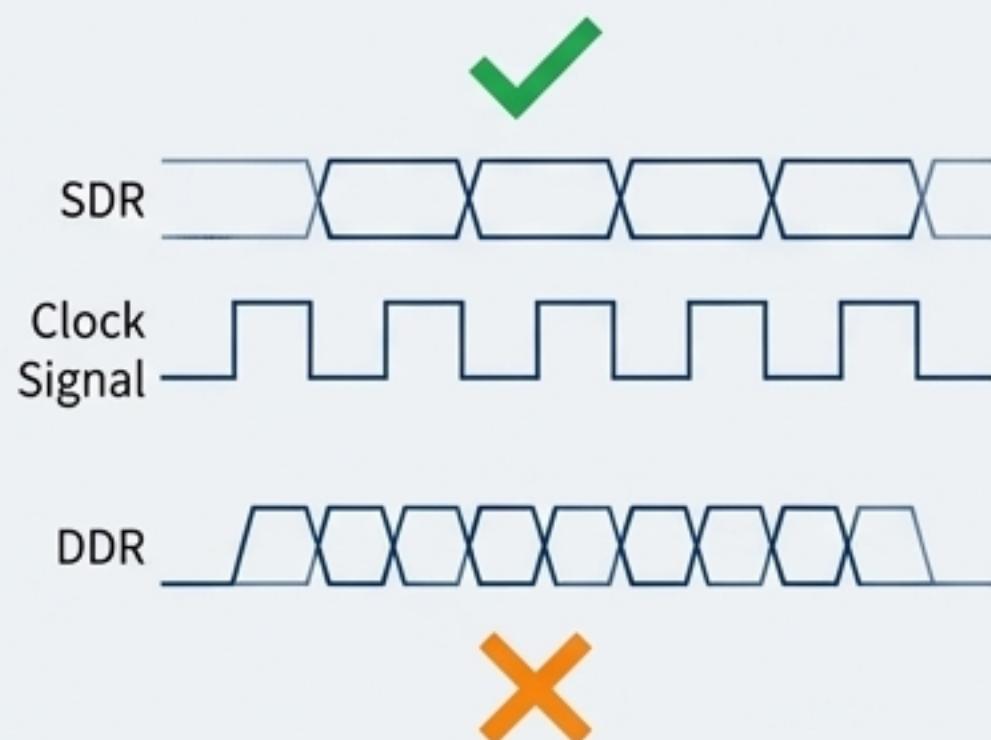
✿ 協議規則 #1: 傳輸結構

CMD42 的指令結構與匯流排事務類型與 **Single Block Write** 指令相同。



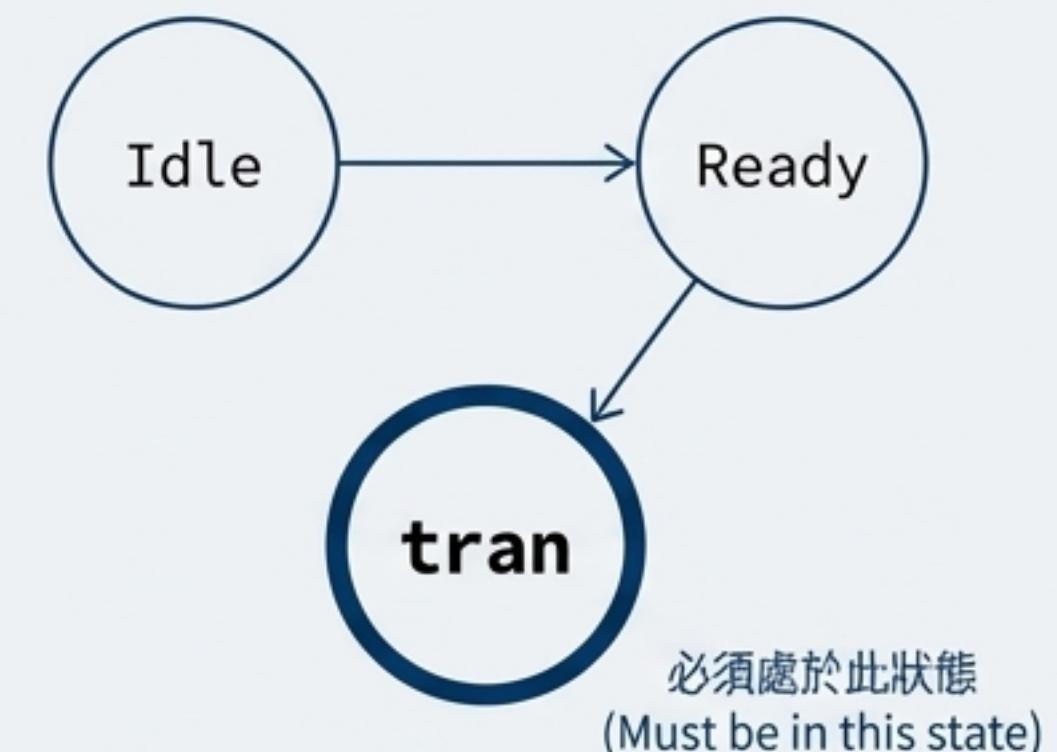
✿ 協議規則 #2: 速度限制

極度重要：此指令 **僅能在 Single Data Rate (SDR) 模式下執行**。在 DDR 模式下發送 CMD42 將被視為非法指令並導致失敗。



✿ 協議規則 #3: 設備狀態

所有鎖定/解鎖相關操作，僅能在設備處於 **Transfer State** 時才能執行。



操作前置作業：發送 CMD42 的標準流程



Step 1: 選中設備 (Select Device)

發送 `CMD7` 並帶上設備的 RCA，以確保指令發送至正確的目標。



Step 2: 設定塊長度 (Set Block Length)

發送 `CMD16 (SET_BLOCKLEN)`。

關鍵：塊長度必須設定為與後續 `CMD42` 資料幀完全相符的大小。

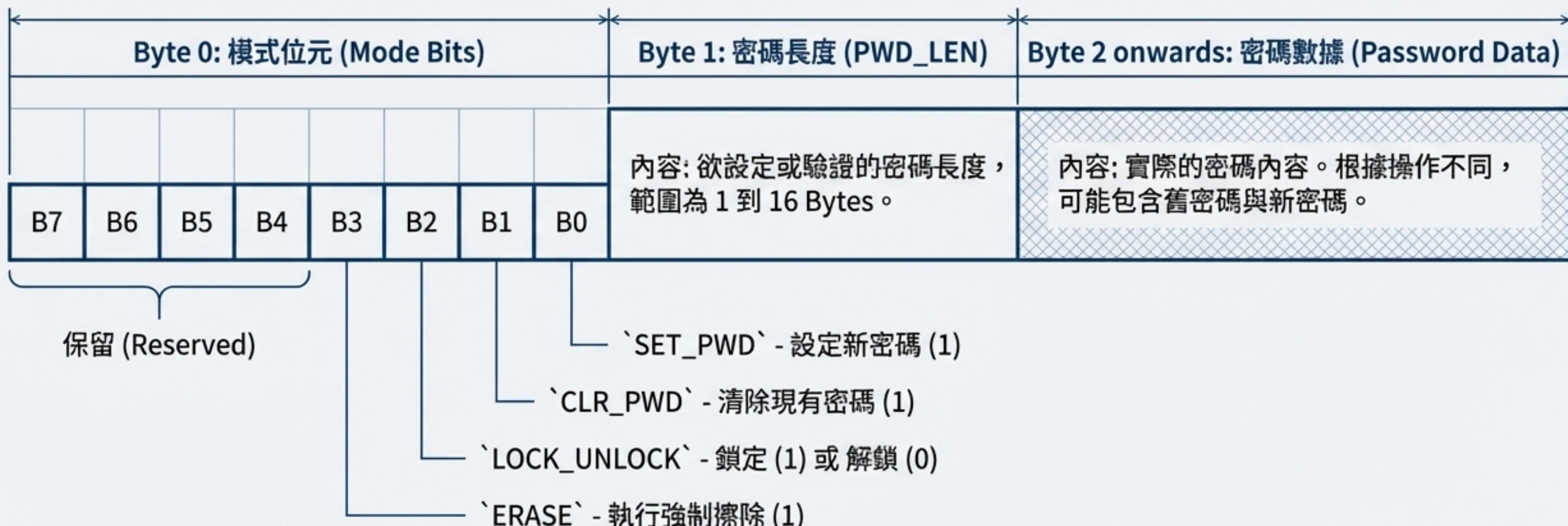
強調 `CMD16` 的設定是確保 `CMD42` 數據能被 eMMC 正確接收與解析的關鍵。



Step 3: 準備就緒 (Ready for CMD42)

執行鎖定/解鎖指令。

解構 CMD42：指令的數據幀藍圖



核心操作 (1/3): 設定與變更密碼

Scenario 1: 首次設定密碼

CMD42 數據幀



指定例 [PultupcØden lis- RtenGf]，首行改產設定密碼。

Scenario 2: 變更現有密碼

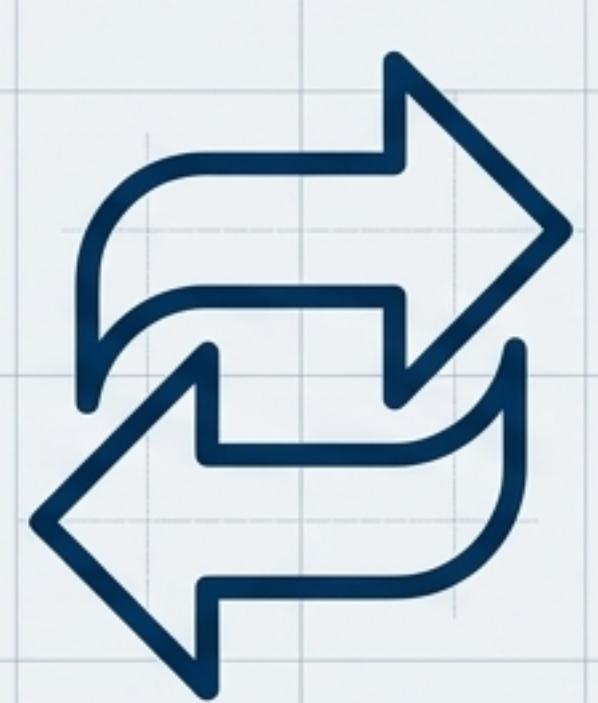
CMD42 數據幀



組合casoating def→ old password，新後密碼和 New password 變更現有密碼。

核心操作 (2/3): 執行鎖定與解鎖

To LOCK the Device

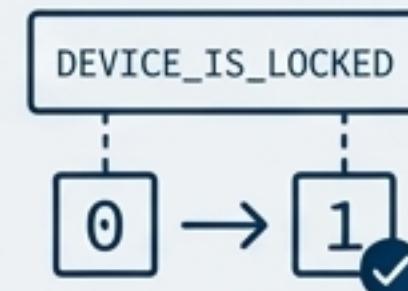


Technical Data Frame

- Byte 0 : LOCK_UNLOCK 位元設為 **1**。
- Byte 1 : 現有密碼的長度 (PWD_LEN)。
- Byte 2+ : 正確的密碼數據。

驗證

操作成功後，可讀取 Device Status，其中的 **DEVICE_IS_LOCKED** 位元會被置位 (set to 1)。



To UNLOCK the Device

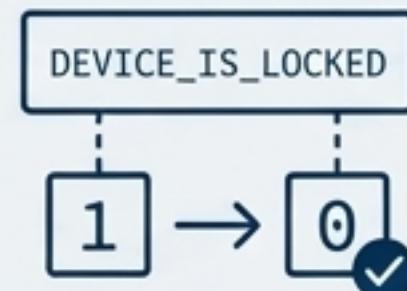


Technical Data Frame

- Byte 0 : LOCK_UNLOCK 位元設為 **0**。
- Byte 1 : 現有密碼的長度 (PWD_LEN)。
- Byte 2+ : 正確的密碼數據。

驗證

操作成功後，**DEVICE_IS_LOCKED** 狀態會被清除。



核心操作 (3/3): 清除密碼

Purpose: 將設備恢復至未設定密碼的狀態。

CMD42 數據幀

- Byte 0: CLR_PWD 位元設為 **1**。
- Byte 1: 現有密碼的長度 (PWD_LEN)。
- Byte 2+: 必須提供正確的現存密碼以供驗證。

Result on Success

- 密碼被清除。
- PWD_LEN 暫存器會被**重置為 0**。



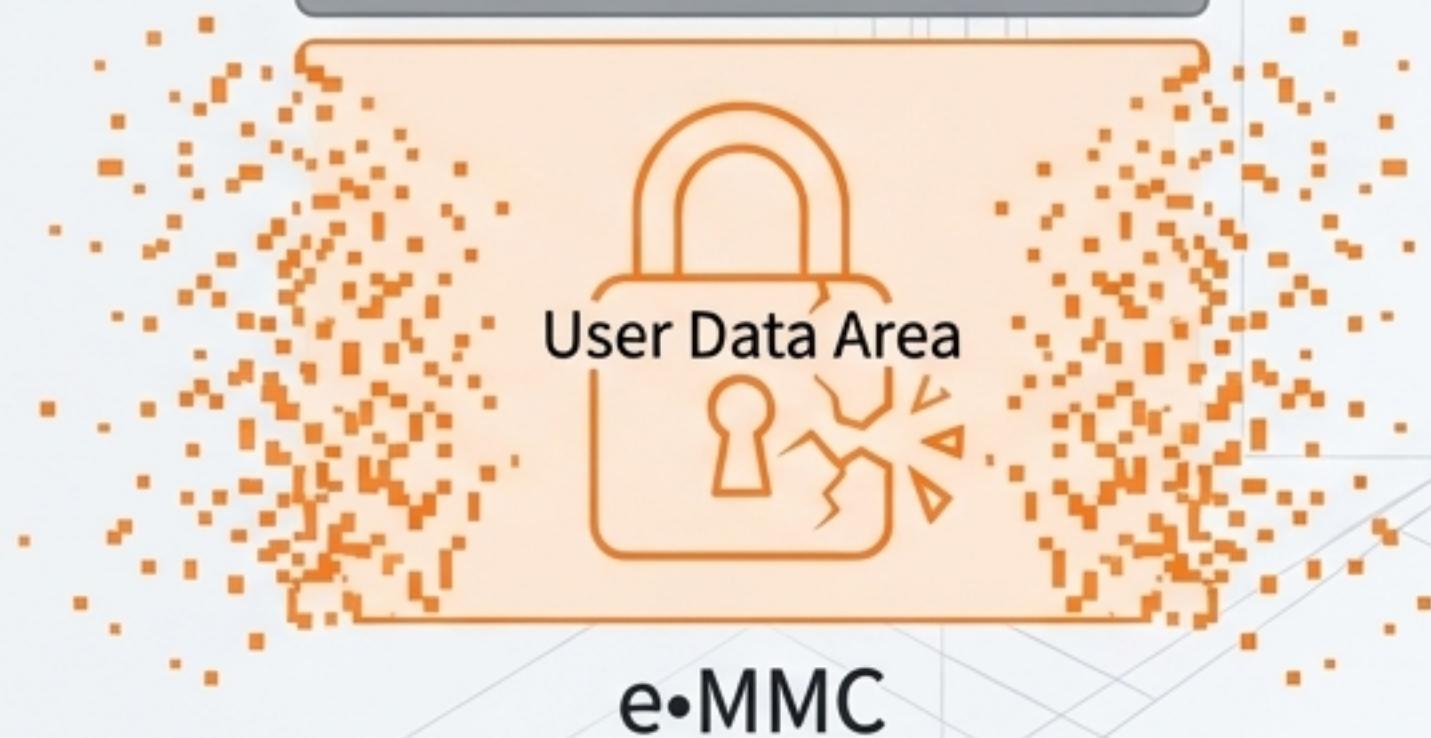
忘記密碼的對策：強制擦除 (Forced Erase)

- 當密碼遺失時，這是唯一的官方恢復方法。此操作會清除所有受保護的內容並解除鎖定。
- How to Trigger
 - 發送一個特殊的 CMD42 數據幀。
 - Byte 0：將 ERASE 位元設為 1。
 - 重要**：SET_PWD、CLR_PWD、LOCK_UNLOCK 位元必須為 0。
 - 此操作 **不需要提供密碼**。
- Scope of Erasure
 - 僅擦除 User Data Area 的數據。
 - 不會影響 Boot Partitions, RPMB, GPPs。

BOOT Partitions

RPMB

GPPs



類比：終極爆破

如果你弄丢了鑰匙，唯一的辦法就是炸掉整個倉庫（清空 User Data Area 的數據），這樣大門才會自動彈開讓你重新設定。

強制擦除的關鍵限制與風險

寫入保護衝突 (Write-Protection Conflict)

若 User Data Area 中存在任何被設定為「永久性寫入保護 (Permanent Write Protection)」或「上電後寫入保護 (Power-On Write Protection)」的區塊，強制擦除指令將會失敗。

Consequence:

- 擦除操作被中止。
- 數據不會被清除。
- 設備將維持在鎖定狀態。

在啟用永久寫保之前，必須充分考慮其對密碼恢復流程的影響。

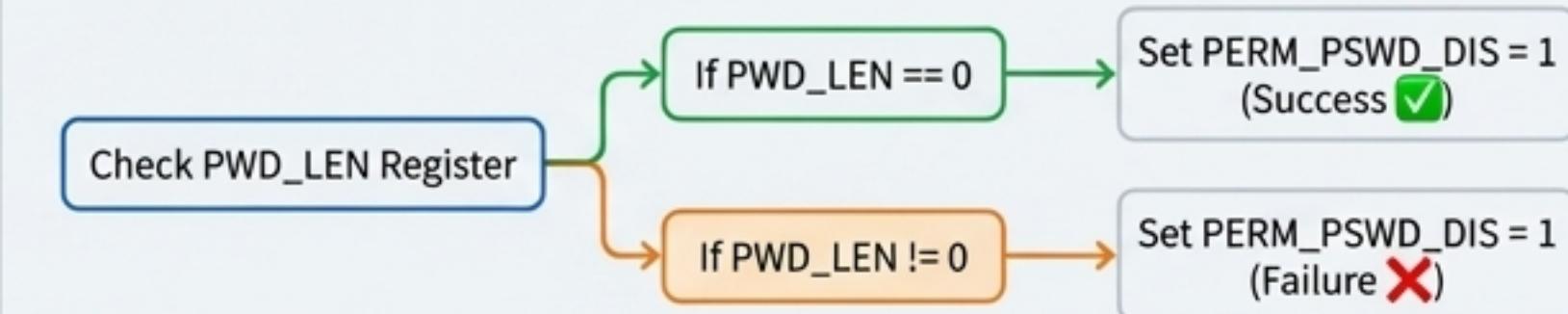




釜底抽薪：永久停用密碼功能

可透過修改 EXT_CSD 暫存器中的 PERM_PSWD_DIS 位元來永久禁用密碼保護功能。

- 將 PERM_PSWD_DIS 位元設為 1。
- 此為一次性操作 (One-Time Programmable)。一旦設定，無法撤銷。



Critical Prerequisite**



此操作僅能在設備當前未設定任何密碼時執行。

若 PWD_LEN 不為 0 (即已有密碼)，試圖設定 PERM_PSWD_DIS 將會失敗。



CMD42 實踐核對清單與關鍵要點

協議要點 (Protocol Essentials)

- SDR Mode Only** : 絶不在 DDR 模式下使用。
- Transfer State** : 確保設備處於 tran 狀態。
- CMD7/CMD16 First** : 永遠先選中設備並設定正確的塊長度。
- Blueprint Reference** : 仔細核對 Byte 0 的模式位元。

架構與安全提醒 (Architecture & Security Notes)

- Scope** : 密碼僅保護 User Data Area。
- Forced Erase** : 會清空用戶數據，但可能因寫保而失敗。
- Permanent Disable** : 永久禁用前，必須先清除現有密碼。
- Status Check** : 始終透過讀取 DEVICE_IS_LOCKED 位元來驗證鎖定狀態。