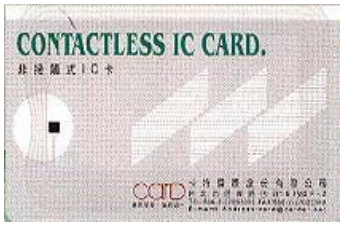
CardWeb®
卡威科技股份有限公司
台北市忠孝東路五段 410 號 5 樓之 2
Tel：(02)2345-4528　Fax：(02)2345-4527
http://www.cardweb.com.tw

產品規格說明

基本資料					
主題名稱	Mifare (RFID：13.56MHz) 非接觸式 IC 卡 S50 完整規格說明				
聯絡人		電話/分機		傳真	
公司名稱		E_mail			
地址					

Mifare 非接觸式 IC 卡片規格說明	
在 Mifare 非接觸式的晶片上客戶可以擁有百分之百的使用權及決定權，屬非接觸式晶片	

安全措施
1.非接觸 IC 卡與讀寫器之間的三重雙向識別 2.數據通信符合 ISO9789-4 3.每一區段均有獨立金鑰，並可於一張卡片上處理多個應用 4.每張卡具有獨立的序號

Mifare 非接觸式 IC 卡片規格表	
項目	規格
Model Name	MIFARE MF1 S50
EEPROM Memory size	1K byte
Independent Sectors	16
Multifunction	Yes
Auti-collision	Yes
Operating Distance	up to 7 cm
Operating Frequency	**13.56Mhz**
Unique Serial Number	Yes
Arithmetic Capability	Increase / decrease
Select Return Code	08h
Default Key Set A	FF FF FF FF FF FF
Default Key Set B	FF FF FF FF FF FF
Single chip	Yes

MIFARE 非接觸式 IC 卡完整技術規格

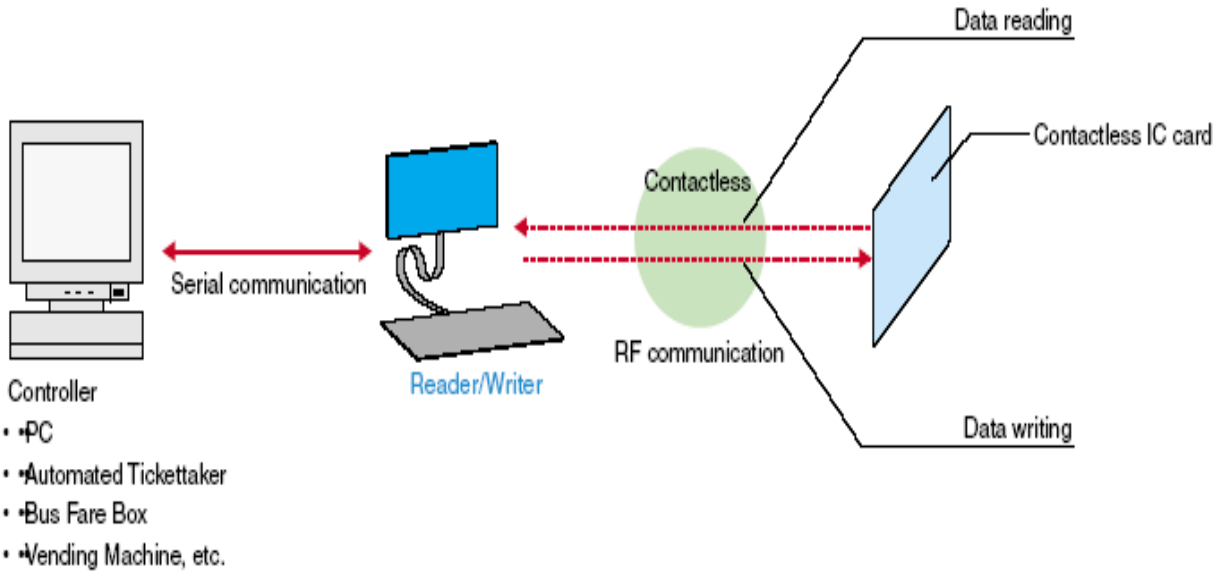
一、概述

MIFARE1 非接觸式 IC 卡是一種可於同一張卡片上處理多種不同應用的非觸式智慧卡，這種將晶片安裝於卡片上，不需接觸即可處理晶片上資料的技術，具備便捷、易用、安全、可靠的特性，特別適合使用在大眾運輸收費系統上，作爲票務的支付工具。以下將針對此卡片的各項特性分別加以說明。

1.1 易用且便捷

MIFARE 非接觸式 IC 卡的大小約和一般的信用卡尺寸相同，在使用此卡處理一筆交易資料時，持卡者僅需將卡片靠近讀寫機即可完成資料的讀取和變更。卡片和讀寫機天線的距離在無阻隔的情況下，約在相隔 100 公釐（100mm）左右即可完成此一筆交易。換言之，持卡人可在同意此某項交易後，將卡片靠近讀寫機來完成此項作業。MIFARE 非接觸式 IC 卡和卡片讀寫機之間經由 106K band 的快速 RF 通訊界面來傳輸資料。

在這個傳輸速度下，一筆一般的交易約可在 0.1 秒內完成，因此當應用此一卡片於大眾運輸系統時，持卡人在經過閘門或公車上下車處時，完全不需等待即可逐一快速通過。MIFARE 非接觸式 IC 卡的尺寸和一般的信用卡尺寸相同，在使用此卡時可將卡片置於皮包內，不需拿出即可使用，即使皮包內放有硬幣也不影響其功能。



1.2 辨識能力

在實際的應用上，經常會遇到多張卡同時進入讀寫機讀寫區域的狀況，例如，當在同一個皮包中放了多張的非接觸式 IC 卡就會產生情形這種。這時讀寫機和卡片間即會執行一個辨識程序，以避免多張卡片同時傳送資料或是一張新進入讀寫區域的卡片干擾了讀寫機和正在處理中卡片間之通訊。此一辨識程式可以讓卡片和卡片讀寫機間之通訊得以確保其通訊之可靠。

卡威科技股份有限公司
TEL：(02)2345-4528 FAX：(02)2345-4527
http://www.cardweb.com.tw

1.3 資料安全

非接觸式 IC 卡提供以下之設計來確保卡片資料的安全：每張卡片均有一個獨一且無法變更的序號。卡片與讀寫機間之相互認證。

1.4 資料加密傳送

每筆資料均加密檢查。

1.5 卡片多用途

非接觸式 IC 卡內之記憶體可分別設定獨立之金鑰和存取權限，這一種記憶體結構可同一張卡片上，設定各個應用程式的記憶體空間和其控管方式來擴展張卡片之應用。

1.6 可靠性

MIFARE 非接觸式 IC 卡是由一線圈和一個晶片封裝於塑膠卡片中而成，此一卡片沒有任何會移動的機構，沒有外部的接點，也不需外加電池，以這種簡單的構造組成的卡片，在使用上其可靠性是無庸置疑的。

1.7MIFARE 系統特性

(1)操作頻率： 13.56 MHz
(2)傳輸速度： 106 k baud
(3)辨識功能： 同時可處理多張卡片
(4)操作距離： 可達 100mm （依天線形狀大小而定）
(5)通訊協定： 半雙工傳輸，交握式協定

1.8 資料傳輸之功能包括：

(1)辨識功能
(2)16-bit CRC 檢查碼
(3)16-bit 同位元檢查碼，每一位元組均提供 1-bit 同位元檢查碼
(4)傳輸位元數檢查
(5)傳輸的編碼方式可判定資料爲 0、1 或是無資料
(6)由交握式協定和位元分析來偵測傳輸頻道

1.9 一卡多用途的支援包括：

(1)辨識功能同時可處理多張卡片。
(2)多張卡片分別進出讀寫區域時，系統會自動分辨以避免讀寫錯誤。
(3)資料讀寫穩定性 當一特定的卡片正在讀寫資料時，其它卡片進出讀寫區域並不會產生干擾。
(4)快速辨識程式 在讀寫區域中，每多一張卡片對一單交易的處理時間僅會增加 1.0 ms。

1.10 MIFARE 非接觸式 IC 卡

(1)卡片材質： PVC （不透光）
(2)卡片尺寸： 符合 ISO 10536
(3)操作溫度： -20℃至+50℃（相對濕度 95%）

卡威科技股份有限公司
TEL：(02)2345-4528 FAX：(02)2345-4527
http://www.cardweb.com.tw

(4)電源： 由無線電傳送，不需外加電池
(5)晶片製程： CMOS EEPROM 製程
(6)卡片組成： 單晶片外加一組線圈

1.11 資料安全

(1)符合 ISO/IEC DIS9789-2 認證程序
(2)無線傳輸之資料均加密傳送，並可防止資訊複製型式之侵入
(3)每一區段（SECTOR）均有獨立的金鑰，可於一張卡片上處理多個應用。
(4)每張卡片均有獨一的序號
(5)具備金鑰傳輸用之金鑰（Transport key）

1.12 卡片用途的記憶體結構

(1)記憶體共 8k Bit ，EEPROM，不需外加電池
(2)記憶體共分成獨立的 16 個區段（Sector），可供多個應用系統分別使用不同之區段。
(3)每一區段（sector）由 4 個區塊（block）所組成。
(4)每一區塊（block）爲讀寫的基本單位，每一區塊共有 16 個位元組（byte）。
(5)每一區段（sector）有自己的金鑰和存取權限，可以以此架構來達到階層式的金鑰系統。
(6)每一個區段均可自行訂定其存取權限。
(7)提供數值區塊（value block）之功能和增減之運算。
(8)資料可保有存達 10 年之久。

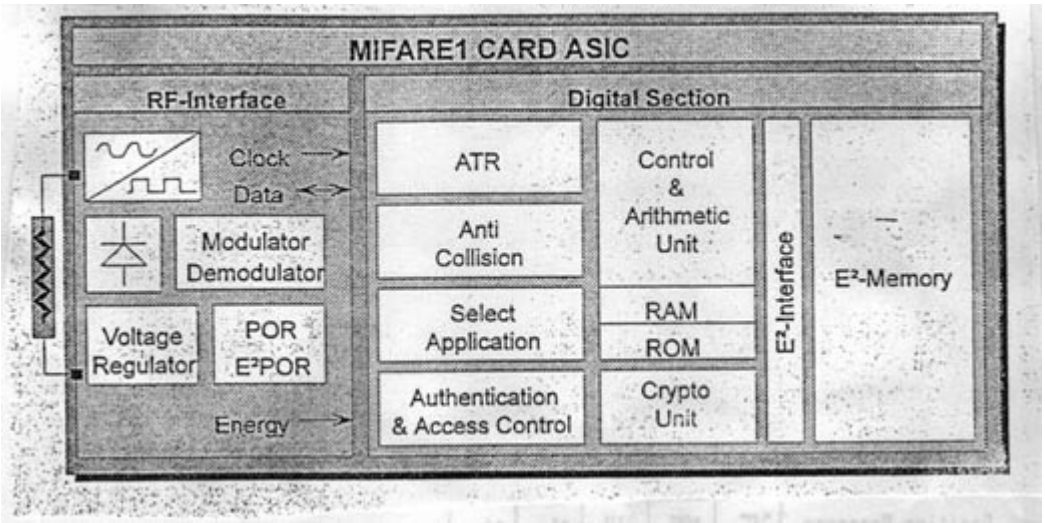
1.13 處理速度

(1)辨識一張卡片 3ms （Answer to Request & Anticollision）
(2)讀取一個區塊（16bytes） 2.5ms （不需認證）
(3)4.5ms （需先認證）
(4)寫入一個區塊並讀取之 9ms （不需認證）
(5)11ms（需先認證）
(6)一般的收費交易 小於 100ms，包括：
(7)辨識卡片，讀取 6 個區塊（768bit 和執行兩個區段的認證），寫入 2 個區塊（256bit）及資料的備份處理。
(8)可對移動中的卡片執行前述動作。

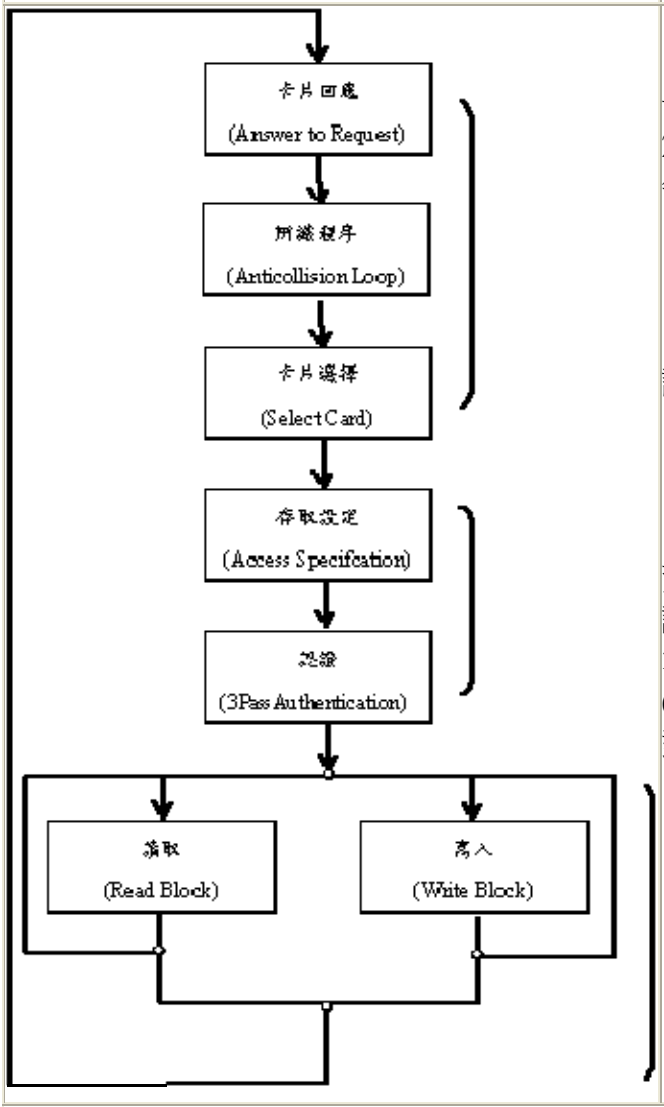
卡威科技股份有限公司
TEL：(02)2345-4528 FAX：(02)2345-4527
http://www.cardweb.com.tw

二、系統方塊圖

2.1Mifare Card ASIC



2.2 非接觸式 IC 卡和讀寫機間之通訊界面方塊圖

交易程序：	執行所需時間(參考值)
	卡片辨識： 2.5 ms 一單一卡片 每增加一張卡片需增加 1 ms 認證：2 ms 資料讀寫： 讀取一個區塊(Block)：2.1ms 寫入一個區塊(Block) ：6 ms (不包含寫入後再讀出和比對)

卡威科技股份有限公司
TEL：(02)2345-4528 FAX：(02)2345-4527
http://www.cardweb.com.tw

(1)卡片回應（Answer to Request）：卡片在進入讀寫機之讀取區域時，會因應讀寫機的指令送出卡片回應訊息，卡片回應訊息主要可用來決定卡片的型態並因而設定卡片與讀寫機間的通訊協定，傳輸速度等參數，以建立其間的通訊。

(2)辨識程序（Anticollision loop）： 在卡片送出卡片回應訊息後；就開始辨識程序以讀取卡片中的序號。當有多張卡片且同時在讀寫機的讀取區域時，辨識程序可依據卡片上的序號來選取其中的一張以執行爾後的認證和讀寫等動作，其它未被選取的卡片則回到等待狀態等待下一次的卡片回應和辨識程序。

(3)存取設定（Access Specification）：在辨識程序選取了某張卡片並取得卡片的序號後，下一個步驟就是指定卡片中所要讀寫的記憶體位置，指定記憶體位置後，才開始執行認證程序。

(4)認證程序（3-Pass Authentication）： 認證程序是要讀寫卡片上某一記憶體位置前所需完成的程序之一。卡片的記憶體必需在認證程序通過後，才可依據此記憶原先設定的存取權限加以讀寫。另外當認證程序完成後，爾後之資料傳輸均將依照 Strean cipher encryetion 的方式加密傳送。

2.3 資料完整性

爲了確保卡片和讀寫機間的資料傳送能夠可靠無誤，在資料的傳送上提供了下朮的功能：辨識處理

2.4 資料安全性

卡片和讀寫機之間的資料安全處理程序包括下列之功能：

(1)符合 ISO-9798-2 之認證程序
(2)資料傳輸加密處理
(3)Stream cipher 加密方法
(4)亂數產生器
(5)每張卡片均有一個不重覆的序號
(6)長度爲 48 位元的金鑰

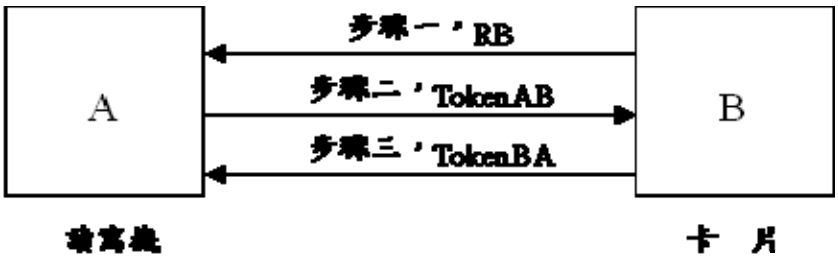
而卡片上之記憶體均需經過認證程序檢證後才可讀寫應用程式也需要知道交付金鑰（Transport key）和卡片上記憶體分成固定大小的區域，每一區域各自擁有其認證所需的金鑰，此種架構對於在一張卡片上放置多個應用系統的資料來說會是非常需要的。

卡片記憶體的一個基本控管區域爲一個區段（sector），一個區段的控制包括兩組金鑰（分別稱之爲金鑰 A 和金鑰 B）和可更改的存取權限。這兩組金鑰和存取權限可用來組成階層式金鑰來管理不同區段的存取方式。在金鑰的應用上，我們可以設定金鑰 A 擁有扣除數值的能力，而金鑰 B 則具有增加數值的能力，增加的功能一在應用系統上一般而言是應管制得更爲嚴密的功能。

卡威科技股份有限公司
TEL：(02)2345-4528 FAX：(02)2345-4527
http://www.cardweb.com.tw

階段認證程序：

認證程序可圖示說明如下：



其中 TokenAB 和 TokenBA 之值爲：
TokenAB = eKAB (RA || RB || B || Text2)
TokenBA = eKAB (RB || RA || Text4)
在 TokenAB 中，參數 B 是用來防止所謂的"重送式攻擊"方法。重送式攻擊是說一個入侵此一系統的人以重
送 RB 的方法來攻擊此一系統，以讓卡片(B)認爲他是 A 無誤。

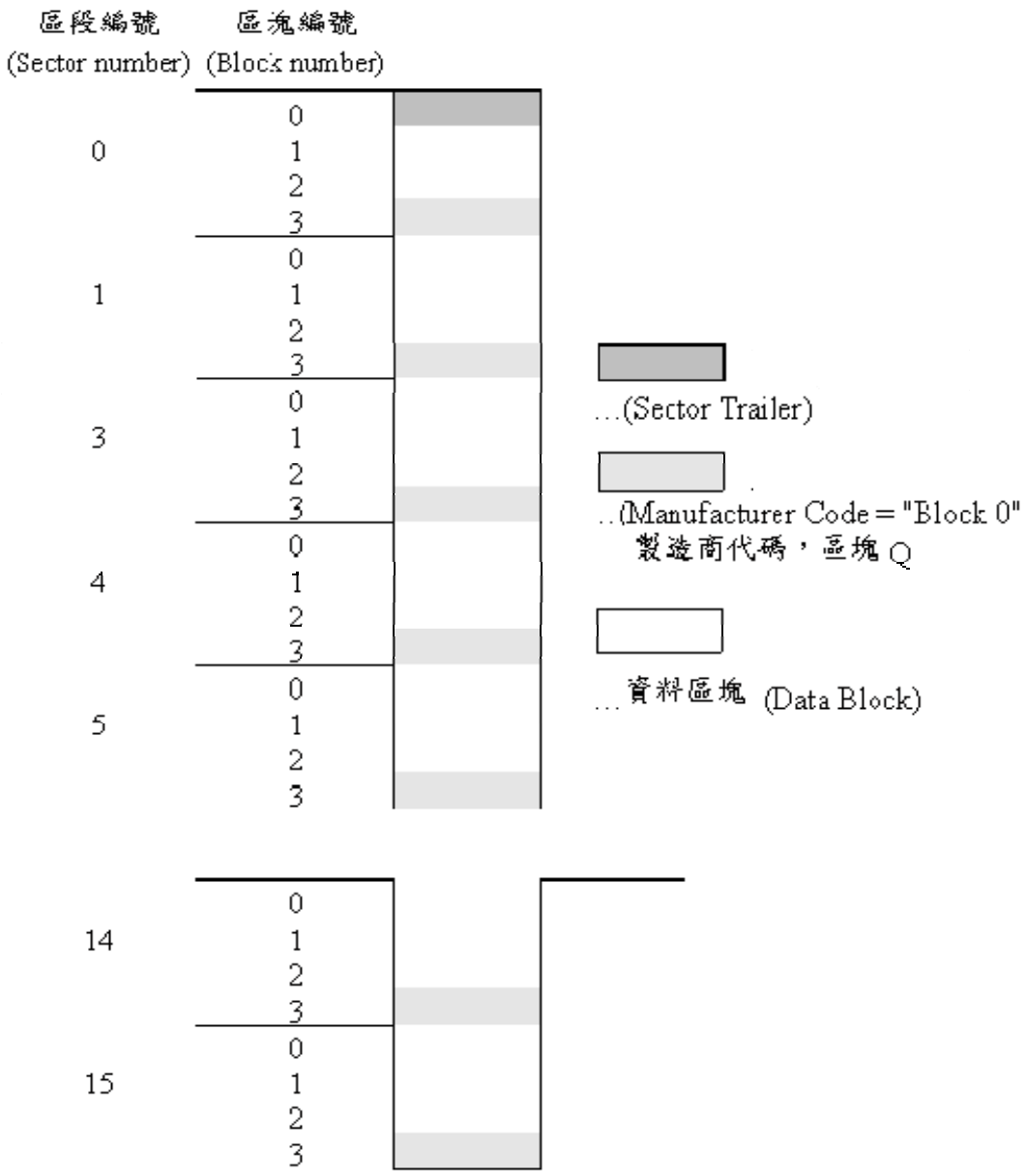
此一認證程序可說明如下：
步驟一： B 端產生一個亂數 RB 送至 A 端。
步驟二： A 端將收到的亂數 RB 依上述之公式產生 TokenAB 並送回 B 端。
步驟三： B 端收到 TokenAB 後，將其加密之部份解回原文，比較參數 B，亂數 RB。同時並根據收到的亂
數 RA，依照上述之公式產生 TokenBA 送回 A 端。
步驟四： A 端收到 TokenBA 後，將其加密部份解回原文，比較亂數 RB，RA 與 TokenBA 中解出之 RB，RA 是
否相符。

2.5 記憶體結構和存取權限

MIFARE 1 非接觸式 IC 卡內之記憶體共有 8192 位元(Bit)的 EEPROM，這些空間被分成 16 個區段(sector)，其中每一個區段包含 4 個區塊(Block)，每一個區塊的大小爲 16 個位元組(Byte = 8 Bit)。

記憶體結構：

卡威科技股份有限公司
TEL：(02)2345-4528 FAX：(02)2345-4527
http://www.cardweb.com.tw



2.5.1 區段(Sector)末端(或第三個區塊)

區段末端是指各區段(Sector)的第四個區塊，這個區塊儲存此一區段的控管金鑰 A (KEYSECXA)，金鑰 B (KEYSECXB，可選擇爲金鑰或資料區)此區段各個區塊的存取權限。如果金鑰 B 並不需要做爲金鑰之用，此區段的第四個區塊中最後 6 個位元組即可以用來儲存一般的資料，但即使是做爲資料儲存之用，此 6 個位元組仍可依據存取權限具有金鑰 B 之功能。

存取權限是以 CnXY 表示，如下圖所示。在下圖中，C1XY 至 C3XY 分別表示此一區段中四個區塊各自之存取權限，爲了安全起見 C1XY 至 C3XY 分別各自以不同格式儲存兩次。在存取權限的資料區中的最後一個位元組(BX7 至 BX0)可用來做爲一般資料儲存空間之用。

卡威科技股份有限公司
TEL：(02)2345-4528 FAX：(02)2345-4527
http://www.cardweb.com.tw

位元組	位元 7 6 5 4 0 3 2 1 0									
0	KEYSECXA									
1										
2										
3										
4										
5		位元	7	6	5	4	3	2	1	0
6	存取權限		C2X3_b	C2X2_b	C2X1_b	C2X0_b	C1X3_b	C1X2_b	C1X1_b	C1X0_b
7			C1X3	C1X2	C1X1	C1X0	C3X3_b	C3X2_b	C3X1_b	C3X0_b
8			C3X3	C3X2	C3X1	C3X0	C2X3	C2X2	C2X1	C2X0
9			BX7	BX6	BX5	BX4	BX3	BX2	BX1	BX0
10	KEYSECXB (可選擇)		b 表示爲此位元之負值，例 C1X0_b = INV (C1X0)							
11										
12										
13										
14										
15										

第四個區塊之存取權限 (Y = 3)

C1X3	C2X3	C3X3	KEYSECXA		ACCESS COND		KEYSECXB	
			read	write	read	write	read	write
0	0	0	never	key A | B	key A | B	never	key A | B	key A | B
0	1	0	never	never	key A | B	never	key A | B	never
1	0	0	never	key B	key A | B	never	never	key B
1	1	0	never	never	key A | B	never	never	never
0	0	1	never	key A | B	key A | B	key A | B	key A | B	key A | B
0	1	1	never	key B	key A | B	never	never	key B
1	0	1	never	never	key A | B	never	never	never
1	1	1	never	never	never	never	never	never

註："Key A | B" 表示 Key A 或 Key B 擇一即可。

卡威科技股份有限公司
TEL：(02)2345-4528 FAX：(02)2345-4527
http://www.cardweb.com.tw

第一至第三個區塊的存取權限 (Y = 0 至 2)

C1XY	C2XY	C3XY	Read	Write	Incr	Decr, transfer, restore
0	0	0	KEY A|B	KEY A|B	KEY A|B	KEY A|B
0	1	0	KEY A|B	NEVER	NEVER	NEVER
1	0	0	KEY A|B	KEY B	NEVER	NEVER
1	1	0	KEY A|B	KEY B	KEY B	KEY A|B
0	0	1	KEY A|B	NEVER	NEVER	KEY A|B
0	1	1	KEY B	KEY B	NEVER	NEVER
1	0	1	KEY B	NEVER	NEVER	NEVER
1	1	1	NEVER	NEVER	NEVER	NEVER

註：incr，decr，transfer 和 restore 之功能是由卡片上之晶片所執行。

交付時之設定

卡片在交付時，金鑰 A 和存取權限的設定值爲：

C1X0，C2X0，C3X0=000

C1X1，C2X1，C3X1=000

C1X2，C2X2，C3X2=000

C1X3，C2X3，C3X3=001

金鑰 A：製造商設定後直接交付予買方。

出廠代碼（區段0內之區塊0）

此一區塊亦稱之爲區塊0（"Block 0"），區塊僅能讀取，其中儲存長度爲 32 位元之出廠代碼。

資料用區塊（除了區塊0之外的第一至第三個區塊）資料用區塊可依據此區段之存取權限，於其內執行下述之功能：

讀取
寫入
數值加入
數值減除
資料存入
資料還原

在 MIFARE1 之非接觸式 IC 卡中區塊可定義爲以下兩種不同的用途：

卡威科技股份有限公司
TEL：(02)2345-4528 FAX：(02)2345-4527
http://www.cardweb.com.tw

一般區塊

一般區塊可用來讀寫及儲存資料。在一個區塊中，建議使用其中的二個元位組做爲此 16 個位元組之讀寫完成狀態之用，此方式可做爲資料備援和寫入失敗時設計上之參考。

數值區塊

數值區塊可用於電子商務之應用，此區塊可使用讀取、數值加入、數值減除、資料存入和資料還原等功能。下爲此區塊之組成圖，其中一個數值是以個位元組表示，此一數值並與其負值分別儲存三次以提供錯誤時更正之能力。

2.5.4 金鑰的管理和多種應用的共存

MIFARE1 非接觸式 IC 卡記憶體的結構可符合多種應用使用之需求，不同的應用可使用不同的區段，並以其控管的金鑰防止資料意外的遭其它應用變更。各區段的金鑰也只有在讀寫機依據卡片之存取權通過金鑰 A 或金鑰 B 之認識後才能加以變更。在沒有完成認證程序的情況下，金鑰或存取權限是無法修改的。

卡片交付時，其金鑰和存取權限已由卡片製造商存入卡片中。

注意：

在變更卡片內之金鑰或存取權限時，需注意在變更未完成前不可將卡片移出讀寫機之讀寫有效區域，以免造成金鑰或有取權限內容錯誤使得此一區段可能無法再加以使用。

2.5.5 資料安全上之考慮

在存取權限中，可設定金鑰 B 其重要性高於金鑰 A，但在通過金鑰 A 的認證程序後，仍可將金鑰 B 之內容讀出。應用系統在設計時需就資料安全方面考慮此一問題所造成之影響。

當金鑰 B 之位置用以儲存一般的資料時，此一區段建議僅用來做爲非放敏感性的一般資料儲存之用，這類的設定建議勿使用在有安全考量的應用上。

卡威科技股份有限公司
TEL：(02)2345-4528 FAX：(02)2345-4527
http://www.cardweb.com.tw