Mifare 1 非接触 IC 卡技术说明

1 特性

1.1 MIFARE RF 接口 (ISO/IEC 14443 A)

- 非接触数据传输并提供能源（不需电池）
- 工作距离：可达 100mm （取决于天线尺寸结构）
- 工作频率：13.56 MHz
- 快速数据传输：106 kbit/s
- 高度数据完整性保护：16 Bit CRC，奇偶校验，位编码，位计数
- 真正的防冲突
- 典型票务交易： < 100 ms （包括备份管理）

1.2 EEPROM

- 1 Kbyte，分为 16 个区，每区 4 个块，每块 16 字节。
- 用户可定义内存块的读写条件
- 数据耐久性 10 年
- 写入耐久性 100.000 次

1.3 安全性

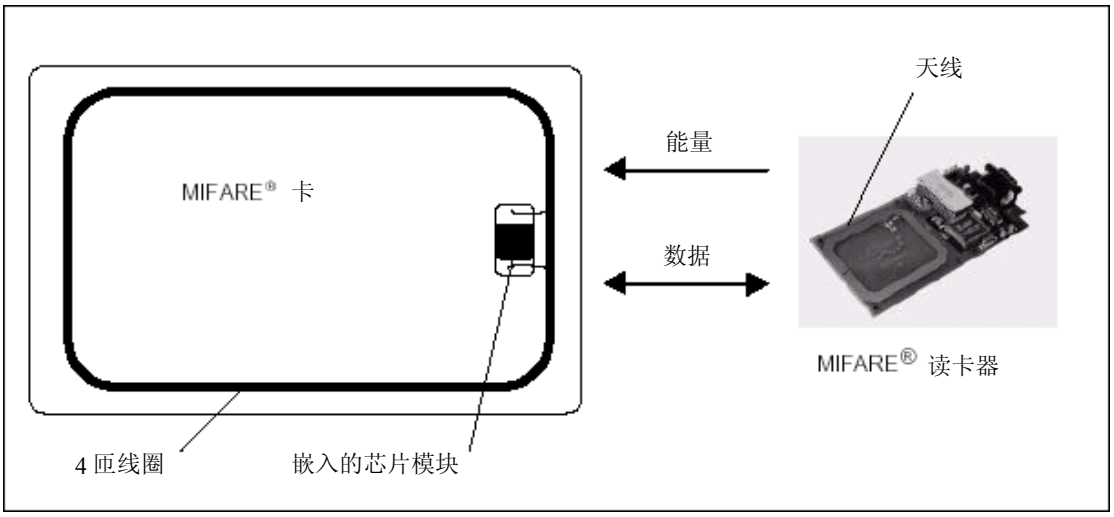
- 相互三轮认证（ISO/IEC DIS9798-2）
- 带重现攻击保护的射频通道数据加密
- 每区（每应用）两个密钥，支持密钥分级的多应用场合
- 每卡一个唯一序列号
- 在运输过程中以传输密钥保护对 EEPROM 的访问权

2 概述

MIFARE MF1 是符合 ISO/IEC 14443A 的非接触智能卡。其通讯层（MIFARE RF 接口）符合 ISO/IEC 14443A 标准的第 2 和第 3 部分。其安全层支持域检验的 CRYPTO1 数据流加密。

2.1 非接触能源和数据传递

在 MIFARE 卡中，芯片连接到一个几匝的天线线圈上，并嵌入塑料中，形成了一个无源的非接触卡。不需要电池。当卡接近读写器天线时，高速的 RF 通讯接口将以 106 kBit/s 的速率传输数据。



2.2 防冲突

智能的防冲突功能可以同时操作读写范围内的多张卡。防冲突算法逐一选定每张卡，保证与选定的卡执行交易，不会导致与读写范围内其他卡的数据冲突。

2.3 用户便捷性

MIFARE 是针对用户便捷性优化的。例如，高速数据传输使得完整的票务交易在不到 100 ms 内处理完毕。因此用户不必在读写器天线处停留，形成高的通过率，减少了公共汽车的登车时间。在交易时，MIFARE 卡可以留在钱包里，甚至钱包里有硬币也不受影响。

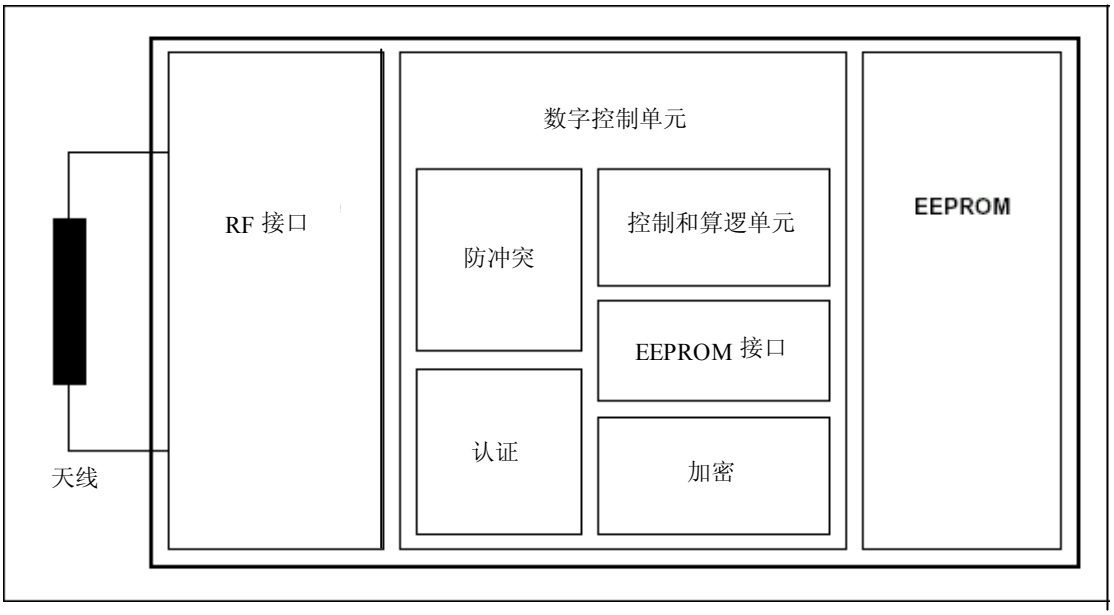
2.4 安全

安全的重点是防欺诈。相互随机数和应答认证、数据加密和报文鉴别检查和，防止各种破解和篡改，使其更适于票务应用。不可更改的序列号，保证了每张卡的唯一性。

2.5 多应用功能

MIFARE 提供了可以与 CPU 卡媲美的真正多应用功能。每区两个不同的密钥支持采用分级密钥的系统。

3 功能说明



3.1 方框图说明

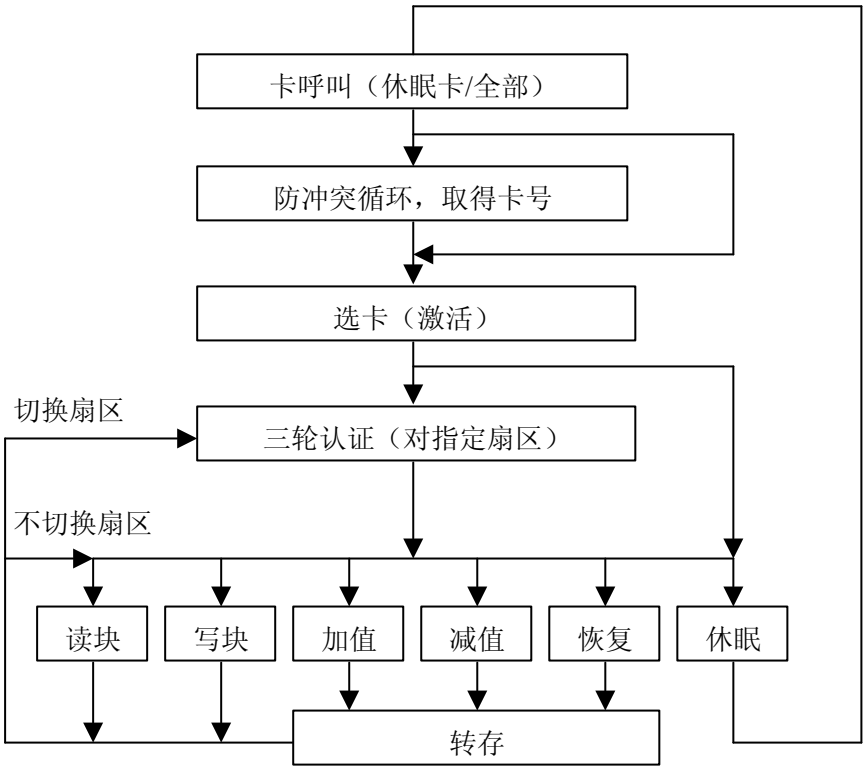
MF1 S50 集成电路芯片内含 1 Kbyte EEPROM、RF 接口和数字控制单元。能量和数据通过天线传输，卡中天线为几匝线圈，直接连接到芯片上。.不再需要额外的组件。

- RF 接口：
  - 调制解调器
  - 检波器
  - 时钟发生器
  - 上电复位
  - 稳压器
- 防冲突：读写范围内的几张卡可以逐一选定和操作。

- 认证：在所有存储器操作之前进行认证过程，以保证必须通过各块指定的密钥才能访问该块。
- 控制和算术逻辑单元：数值以特定的冗余格式存储，可以增减。
- EEPROM 接口
- 加密单元：域验证的 CRYPTO1 数据流加密，保证数据交换的安全。
- EEPROM: 1 Kbyte，分 16 区，每区 4 块。每一块有 16 字节。每区的最后一块称作“尾块”，含有两个密钥和本区各块的读写条件。

3.2 通讯原理

命令由读写器发出，根据相应区读写条件受数字控制单元的控制。



3.2.1 呼叫（REQUEST STANDARD / ALL）

卡上电复位后，通过发送 request 应答码（ATQA 符合 ISO/IEC 14443A），能够回应读写器向天线范围内所有卡发出的 request 命令。

3.2.2 防冲突循环（ANTICOLLISION LOOP）

在防冲突循环中，读回一张卡的序列号。如果在读写器的工作范围内有几张卡，它们可以通过唯一序列号区分开来，并可选定以进行下一步交易。未被选定的卡转入待命状态，等候新的 request 命令。

3.2.3 选卡（SELECT CARD）

读写器通过 select card 命令选定一张卡以进行认证和存储器相关操作。该卡返回选定

应答码（ATS= 08h），明确所选卡的卡型。

3.2.4 三轮认证（3 PASS AUTHENTICATION）

选卡后，读写器指定后续读写的存储器位置，并用相应密钥进行三轮认证。认证成功后，所有的存储器操作都是加密的。

3.2.5 存储器操作

认证后可执行下列操作：

- 读数据块
- 写数据块
- 减值：减少数据块内的数值，并将结果保存在临时内部数据寄存器中。
- 加值：增加数据块内的数值，并将结果保存在数据寄存器中。
- 恢复：将数据块内容移入数据寄存器。
- 转存：将临时内部数据寄存器的内容写入数值块。

3.3 数据完整性

在读写器和卡之间的非接触通讯链接中实施下列机制，以保证数据传输的可靠性：

- 每块 16 bit CRC
- 每字节的奇偶位
- 位计数检查
- 位编码，以区分”1”、 ”0”和无信息。
- 通道监控（协议序列和位流分析）

3.4 安全

采用符合 ISO 9798-2 的三轮认证，以保证高度的安全性。

3.4.1 三轮认证流程

a) 读写器指定要访问的区，并选择密钥 A 或 B。

b) 卡从位块读区密钥和访问条件。然后，卡向读写器发送随机数。（第一轮）

c) 读写器利用密钥和随机数计算回应值。回应值连同读写器的随机数，发送给卡（第二轮）。

d) 卡通过与自己的随机数比较，验证读写器的回应值，再计算回应值并发送（第三轮）。

e) 读写器通过比较，验证卡的回应值。

在第一个随机数传送之后，卡与读写器之间的通讯都是加密的。

3.5 RF 接口

RF 接口符合非接触智能卡标准 ISO/IEC 14443A。

读写器的载波电磁场始终存在（发送中有短暂中断），因为它用作卡的电源。对于两个方向的数据通讯，每个数据帧都只有一个起始位。所传送的每个字节末尾都有一个奇偶校验位（奇校验）。选定块最低地址字节的最低位首先传送。最大帧长为 163 bit（16 数据字节 + 2 个 CRC 字节 = 16 * 9 + 2 * 9 + 1 起始位）。

3.6 存储器组织

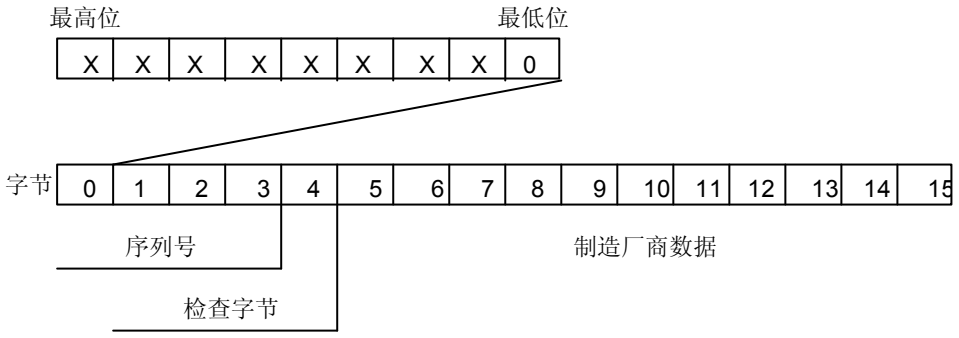
1024 x 8 bit EEPROM 存储器分为 16 区，每区 4 块，每块 16 字节。

在擦处后的状态下，EEPROM 的单元读为逻辑“0”，写后的状态下读为“1”。

扇区	块	块内字节编号 0 1 2 3 4 5 6 7 8 9 A B C D E F	说明
15	3	KEY A 控制位 KEY B	扇区 15 尾块
	2		数据
	1		数据
	0		数据
14	3	KEY A 控制位 KEY B	扇区 14 尾块
	2		数据
	1		数据
	0		数据
⋮	⋮		
1	3	KEY A 控制位 KEY B	扇区 1 尾块
	2		数据
	1		数据
	0		数据
0	3	KEY A 控制位 KEY B	扇区 0 尾块
	2		数据
	1		数据
	0		制造商占用块

3.6.1 厂商代码块

这是第 1 区的第 1 块（块 0）。它含有集成电路制造商数据。出于安全和系统需求，此块是制造商在生产过程中编程后写保护的。



3.6.2 数据块

各区均有 3 个 16 字节的块用于存储数据（区 0 只有两个数据块以及一个只读的厂商代码块）。

数据块可以通过读写控制位设置为：

- 读写块，例如用于非接触门禁管理
- 数值块，例如用于电子钱包，另有可直接控制存储值的命令，如增值、减值。

在任何存储器操作之前必须执行认证命令。

3.6.2.1 数值块

数值块具有电子钱包功能（有效命令：*read, write, increment,decrement, restore, transfer*）。

数值块有固定的数据格式，以便于错误检测、纠错和备份管理。

数值块只能通过以数值块格式的写操作生成：

- 数值：有符号 4 字节数值。数值的最低字节存储在最低地址字节。负值以标准的 2 的补码形式存储。出于数据完整性和安全原因，数值存储三次，两次不取反，一次取反。
- 地址（Adr）：1 字节地址，当进行备份管理时，可用于保存块的地址。地址保存四次。两次取反，两次不取反。在 *increment*、*decrement*、*restore* 和 *transfer* 操作中，地址保持不变。它只能通过 *write* 命令更改。

字节号	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
说明	数值				数值				数值				Adr	Adr	Adr	Adr

3.6.3 尾块（块 3）

各区均有一个尾块，存有：

- 密钥 A 和 B（可选），读时返回逻辑“0”。
- 该区四个块的读写条件，存储在字节 6 至 9 。读写控制位也指定了数据块的类型（读写块或数值块）。

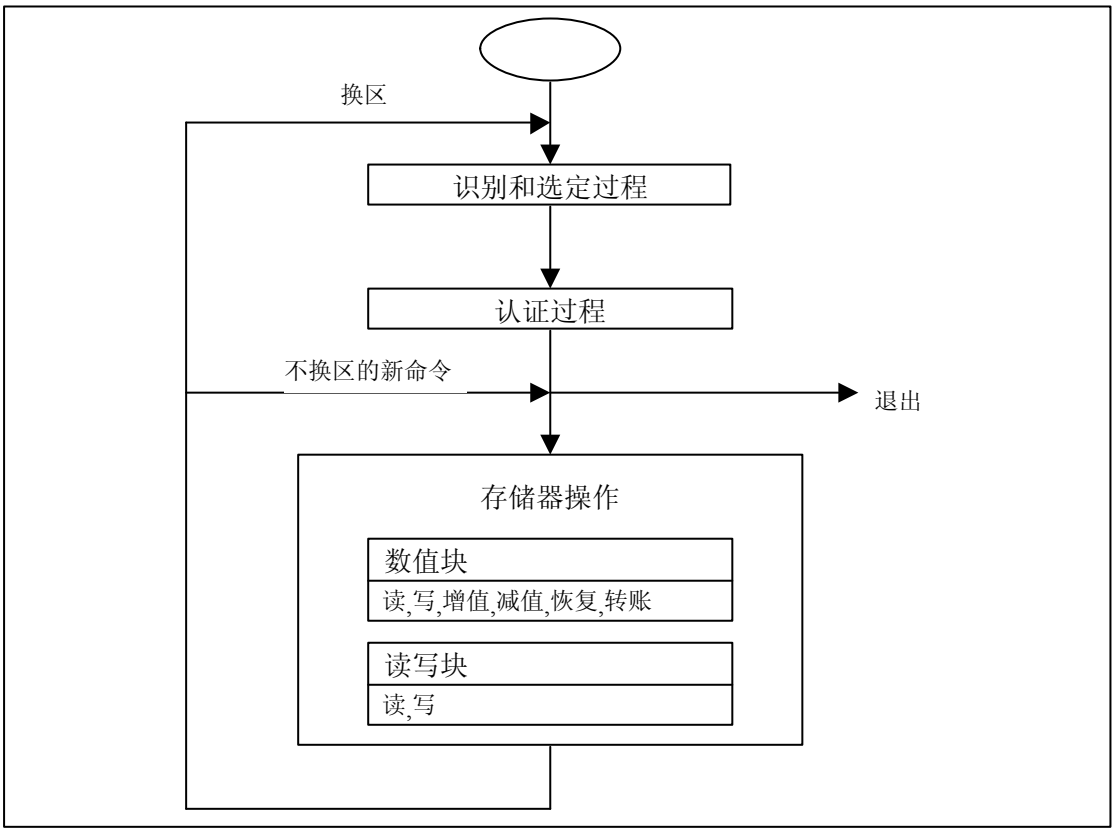
如果不需要密钥 B，块 3 的最后 6 字节可以用作数据字节。

尾块的字节 9 可用于用户数据。因为此字节享有与字节 6、7、8 相同的读写权限。

字节号	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
说明	密钥 A						读写条件				密钥 B（可选）					

3.7 存储器读写

必须如前所述，先选定卡并通过认证，才能执行存储器操作。



存储器操作		
操作	**说明**	**使用块型**
读	读存储器块	读写、数值和尾块
写	写存储器块	读写、数值和尾块
增值	增加块的内容，并将结果存入内部寄存器	数值
减值	减少块的内容，并将结果存入内部寄存器	数值
转存	将内部寄存器内容写入块中	数值
恢复	将块中内容写入内部寄存器	数值

对指定块可以执行的存储器操作取决于所用的密钥和存储在相应尾块中的读写条件。

3.7.1 读写条件

每个数据块和尾块的读写条件均由 3 个 bit 定义，并以非取反和取反形式保存在各个区的尾块中。

读写控制位管理着使用密钥 A 和 B 读写存储器的权限。如果知道相关的密钥，并且当前读写条件允许，读写条件是可以更改的。

读写控制位	**有效命令**		**块**	**说明**
C13 C23 C33	read, write	→	3	尾块
C12 C22 C32	read, write, increment, decrement, transfer, restore	→	2	数据块
C11 C21 C31	read, write, increment, decrement, transfer, restore	→	1	数据块
C10 C20 C30	read, write, increment, decrement, transfer, restore	→	0	数据块

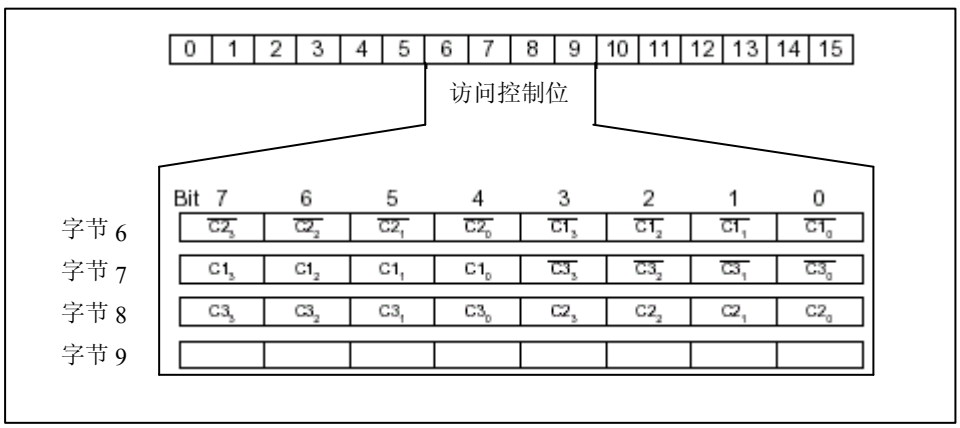
注意：在每一次存储器读写时，内部逻辑会验证存储条件的格式。如果发现个是错误，这个区将被永久性锁死。

注意：在下列说明中，读写控制位是仅以非取反形式表述的。

MF1 的内部逻辑保证了命令只有在通过认证后才被执行。

3.7.2 尾块的读写条件

对密钥和控制位的读写取决于尾块（块 3）的访问控制位，分为“禁止”、“KEY A”、“KEY B”和“KEY A|B”（ KEY A 或 KEY B）。



访问控制位			所控制的访问对象						注释
			KEY A		访问控制位		KEY B		
C1	C2	C3	读	写	读	写	读	写	
0	0	0	禁止	Key A	Key A	Key B	Key A	Key A	Key B 可读
0	1	0	禁止	禁止	Key A	禁止	Key A	禁止	Key B 可读
1	0	0	禁止	Key B	Key A|B	禁止	禁止	Key B	
1	1	0	禁止	禁止	Key A|B	禁止	禁止	禁止	
0	0	1	禁止	Key A	Key A	Key A	Key A	Key A	Key B 可读 传输配置状态
0	1	1	禁止	Key B	Key A|B	Key B	禁止	Key B	
1	0	1	禁止	禁止	Key A|B	Key B	禁止	禁止	
1	1	1	禁止	禁止	Key A|B	禁止	禁止	禁止	

注：灰色行为 key B 可读并可用于存储数据的访问控制条件。

尾块和 key A 被预定义为传输配置状态。因为在传输配置状态下 key B 可读，新卡必须用 key A 认证。

因为访问控制位本身也可以禁止访问，所以个人化时应当特别小心。

3.7.3 数据块的访问控制条件

对数据块（块 0 至 2）的读写访问取决于其访问控制位，分为“禁止”、“KEY A”、“KEY B”和“kEY A|B”（ KEY A 或 KEY B）。相关访问控制位的设置确定了其用途以及相应的可用命令。

- 读写块：允许读、写操作。
- 数值块：运行另外的数值操作——加值、减值、转存和恢复。在用于非充值卡的一种情况（‘001’）下，只能够读和减值。在另一种情况（‘110‘）下，可以用 key B 充值。
- 制造厂商块：只读，不受访位控制位设置的影响！
- 密钥管理：在传输配置状态下，必须用 key A 认证。

访问控制位			所控制的访问操作				用途
C1	C2	C3	读	写	加值	减值 转存 恢复	
0	0	0	key A|B[1]	key A|B[1]	key A|B[1]	key A|B[1]	传输配置状态
0	1	0	key A|B[1]	key B[1]	禁止	禁止	读写块
1	0	0	key A|B[1]	key B[1]	禁止	禁止	读写块
1	1	0	key A|B[1]	key B[1]	key B[1]	key A|B[1]	数值块
0	0	1	key A|B[1]	禁止	禁止	key A|B[1]	数值块
0	1	1	key B[1]	key B[1]	禁止	禁止	读写块
1	0	1	key B[1]	禁止	禁止	禁止	读写块
1	1	1	禁止	禁止	禁止	禁止	读写块

[1] 如果相应扇区尾块 Key B 可读，则不得用作认证（前表中所有灰色行）。**后果：**如果读写器试图用灰色行的访问控制条件以 Key B 认证任何扇区的任何块，卡将在认证后拒绝所有后续存储器访问。