Mifare®标准 IC 卡 MF1 IC S50 功能说明书

目录

1．特征 2
1.1 MIFARE® RF 接口（ISO/IEC 14443A） 2
1.2 EEPROM 2
1.3 保密性（Security) 2
2．总体描述 2
2.1 无线传送数据和能量 2
2.2 反冲突 2
2.3 用户更方便 2
2.4 保密性 3
2.5 多应用功能 3
2.6 发货选项 3
3．功能描述 3
3.1 方框图描述 3
3.2 通讯原理 4
3.2.1 请求标准 / 所有 4
3.2.2 反冲突环 4
3.2.3 选择卡 4
3.2.4 3 轮确认 4
3.2.5 存储器操作 5
3.3 数据可靠（正确）性 5
3.4 保密性 5
3.4.1 3 轮确认的顺序 5
3.5 RF 接口 6
3.6 存储器结构 6
3.6.1 厂商段 6
3.6.2 数据段 7
3.6.3 区尾（段 3） 7
3.7 访问存储器 8
3.7.1 访问条件 9
3.7.2 区尾的访问条件 9
3.7.3 数据段的访问条件 10

1．特征

1.1 MIFARE® RF 接口（ISO/IEC 14443A）

- 无线传送数据和能量（不需要电池）
- 工作距离：最高可达 100mm（由天线的结构（geometry）决定）
- 工作频率：13.56MHz
- 数据传送速度快：106kbit/s
- 数据高度可靠（正确）：16 位 CRC，奇偶校验，位编码，位计数
- 真正的反冲突
- 典型的购票处理（ticketing transaction）：<100ms（包括备份管理）

1.2 EEPROM

- 1K 字节，分成 16 个区，每区又分成 4 段，每一段中有 16 个字节
- 用户可以定义每一个存储器段的访问条件
- 数据可以保持 10 年
- 可写 100,000 次

1.3 保密性（Security)

- 需要通过 3 轮确认（ISO/IEC DIS9798-2）（Mutual three pass authentication）
- RF 信道的数据加密，有重放攻击保护
- 每个区有两套独立的密钥（每应用），支持带密钥层次的多应用（support multi-application with key hierarchy）
- 每个设备有唯一的序列号
- 在运输过程中访问 EEPROM 有传输密钥保护（transport key protects access to EEPROM on chip delivery）

2．总体描述

根据 ISO/IEC 14443A 标准，Philips 开发了无线智能卡芯片 Mifare® MF1 IC S50。这个芯片的通讯层（Mifare® RF 接口）遵从 ISO/IEC 14443A 标准的第 2 部分和第 3 部分。保密层（security layer）使用经区域验证的 CRYPTO1 流密码（field-proven CRYPTO1 stream cipher），使典型 Mifare®系列芯片的数据交换得到保密。

2.1 无线传送数据和能量

Mifare®系统中，MF1 IC S50 连接着几匝线圈（线圈嵌入到塑料中），这就形成了一张无源的无线智能卡。这种卡不需要电池。当智能卡靠近读写装置（Read Write Device，RWD）的天线时，高速 RF 通讯接口可以以 106kBit/s 的速度传送数据。

2.2 反冲突

智能的反冲突功能允许同一工作区域中有不止一张卡同时工作。反冲突算法每次只选择一张卡，确保对被选中的卡正确执行操作而且同一区域中的其他卡不会破坏数据。

2.3 用户更方便

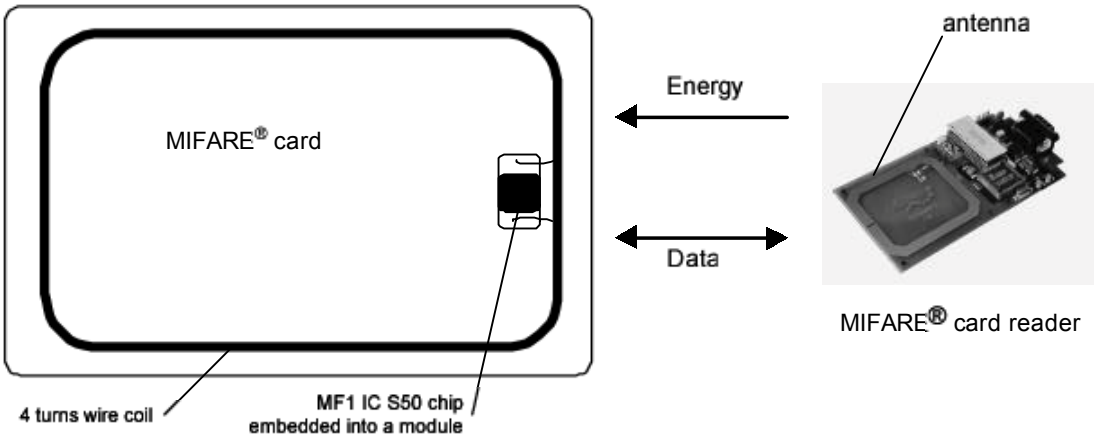
系统的设计使用户更加方便。由于数据传送速率很高，它可以使整个买票过程在小于 100ms 中完成。这样，Mifare®卡用户就不需要停在 RWD 前面，增大了通道（门）的吞吐量，减少了上公共汽车的时间。如果卡放在钱包中（钱包中甚至有硬币）也可以进行交易。

2.4 保密性

这个卡一个特殊的要点是保密，防止欺骗。相互询问（Mutual challenge）和响应确认，数据保密和报文确认检查防止系统受到任何干扰，使购票应用更有吸引力。序列号不可修改，保证了每张卡都是唯一的。

2.5 多应用功能

和处理器卡（processor card）的功能相比较，Mifare®系统提供了一个实时的多应用功能。每区有两个不同的密钥，这样系统可以使用密钥层次。



2.6 发货选项

- 晶片电路
- 突出的晶片电路
- 芯片卡模块

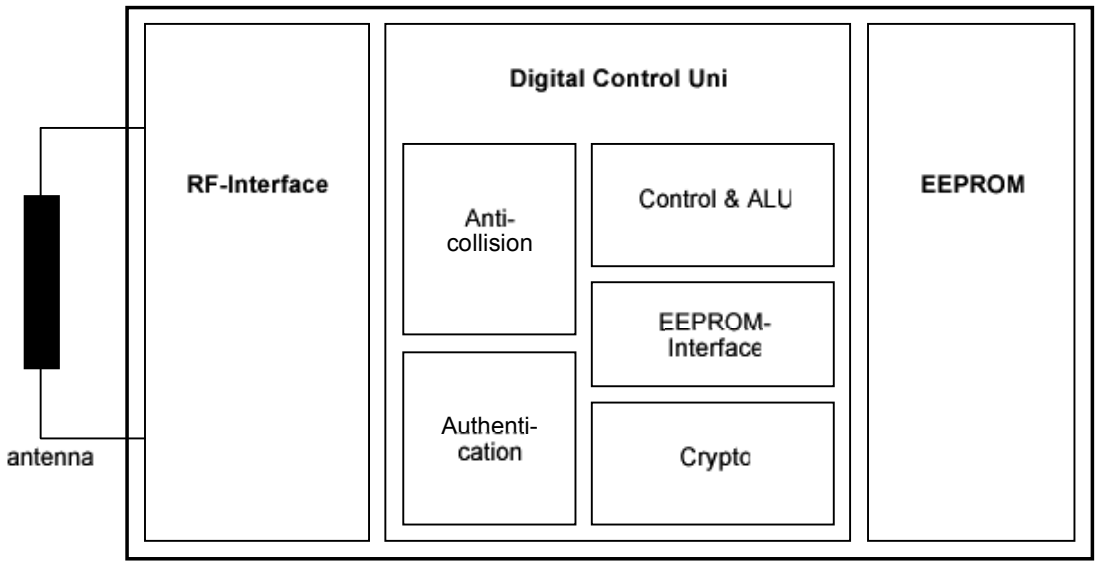
3．功能描述

3.1 方框图描述

MFI IC S50 由 1KB 的 EEPROM、RF 接口和数字式控制单元组成。能量和数据都通过天线传送，天线由几匝线圈组成并直接连到 MF1 IC S50。不需要其他外部元件。（详细的天线设计资料请参考 Mifare® 卡 IC 线圈设计指南）

- RF 接口：
  - 调制器 / 解调器
  - 整流器
  - 时钟再生器（Clock Regenerator）
  - 上电复位
  - 电压调整器
- 反冲突：在同一区域中的卡可以被顺序选中执行操作
- 确认：确认过程确保只有通过每个段的两个密钥才能对这个段进行任何存储器操作。
- 控制和算术逻辑单元：值以特殊的冗余格式（special redundant format）保存，而且可以增加和减少
- EEPROM 接口
- Crypto 单元：Mifare®经典系列经区域验证的 CRYPTO1 流密码（field-proven CRYPTO1 stream cipher）确保数据交换的保密性

- EEPROM：有 1K 字节，分成 16 个区，每区又分成 4 段，每一段中有 16 个字节。每个区的最后一个段叫“尾部”，它包括两个密钥和这个区中每一个段的访问条件（可编程）。



3.2 通讯原理

通讯命令由 RWD 初始化，并由 MF1 IC S50 的数字式控制单元根据相应区的有效访问条件来控制。

3.2.1 请求标准 / 所有

卡上电复位（POR）后，它可以给请求代码发送回应（ATQA，根据 ISO/IEC 14443A）回复 RWD 的请求命令（由 RWD 发出，给所有在天线范围内的卡）。

3.2.2 反冲突环

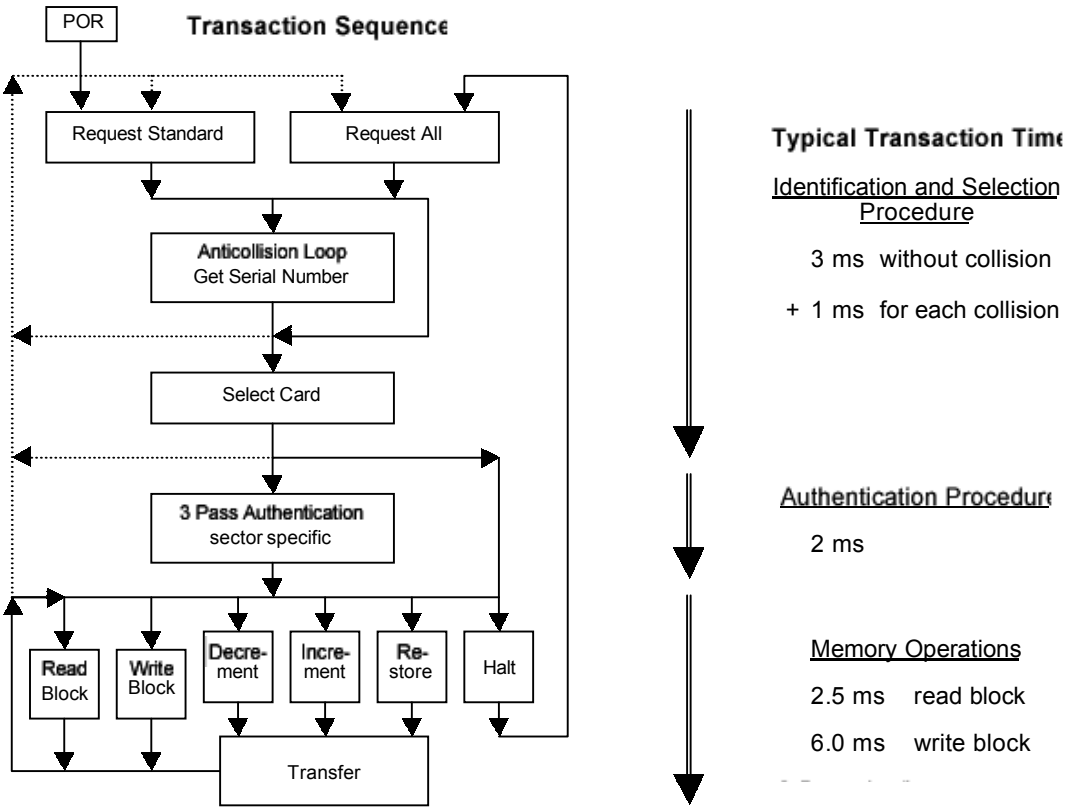
反冲突环可以读出卡的序列号。如果在 RWD 的工作范围内有几张卡，RWD 通过唯一的序列号来区别它们而且每次选择其中一张卡（也叫选择卡）进行下一步操作。没有被选中的卡会回到准备模式等待新的请求命令。

3.2.3 选择卡

RWD 使用选择卡命令选中其中一张卡进行确认和存储器相关操作。卡返回 Answer To Select（ATS）码（=08h），RWD 通过 ATS 可以确定被选中的卡的类型。如果需要更详细的资料请参考 Mifare®标准卡类型识别过程。

3.2.4 3 轮确认

选中了一张卡之后，RWD 指出了接着要访问的存储器位置，然后使用相应的密钥进行 3 轮确认。在成功确认后，所有的存储器操作都是保密的。



3.2.5 存储器操作

确认之后可以执行以下的任何操作：

- 读存储器段
- 写存储器段
- 减：减存储器段的内容并将结果保存在临时的内部数据寄存器中
- 增：增加存储器段的内容并将结果保存在数据寄存器中
- 恢复：将存储器段的内容移到数据寄存器
- 传送：将临时内部数据寄存器的内容写到值存储器段中

3.3 数据可靠（正确）性

RWD 和卡之间的无线通讯链路使用了以下的机制确保数据可靠地传输：

- 每个段 16 位 CRC
- 每个字节都有奇偶校验位
- 位计数检查
- 用位编码区别“1”、“0”和没有信息
- 信道监控（协议序列和位流分析）

3.4 保密性

根据 ISO 9798-2 使用 3 轮确认，保密级别很高。

3.4.1 3 轮确认的顺序

a) RWD 指定要访问的区并选择密钥 A 或密钥 B。

b) 卡从区尾读出密钥和访问条件。然后卡发送一个随机数（作为询问（challenge））到 RWD。（第一轮）

c) RWD 用密钥和附加输入计算响应。然后，将响应和 RWD 的随机询问一起发送到卡中。（第二轮）

d) 卡用自己的询问和 RWD 的响应相比较确认 RWD 的响应。然后卡计算询问的响应并发送出去。（第三轮）（The card verifies the response of the RWD by comparing it with its own challenge and then it calculates the response to chanllenge and transmits it.）

e) RWD 用自己的询问和卡的响应相比较确认卡的响应。（the RWD verifies the response of the card by comparing it to its own challenge）

在发送第一个随机的询问之后，卡和 RWD 之间的通讯是保密的。

3.5 RF 接口

RF 接口是根据无线智能卡标准 ISO/IEC 14443A 设计的。

RWD 的载波区一直存在（在传送时会有短暂暂停），卡的能量从载波区获得。

在两个方向的数据通讯中，在每个帧的开始都有只一个起始位。每个字节在传送时最后都有一个奇偶校验位（奇校验）。所选段最低地址的字节最低位（LSB）被首先发送。最大的帧长度是 163 位（16 个数据字节＋2CRC 字节＝16*9+2*9+1 个起始位）。

3.6 存储器结构

1024x8 位的 EEPROM 存储器被分成 16 个区，每个区中有 4 个段，每段有 16 字节。

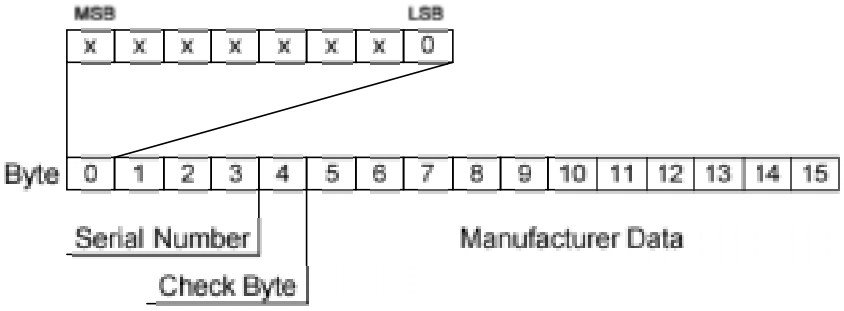
在擦除状态时，读 EEPROM 单元的值是逻辑“0”；在写状态时，读 EEPROM 单元的值是逻辑“1”。

		Byte Number within a Block															
Sector	**Block**	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	**Description**
15	3	Key A						Access Bits				Key B						Sector Trailer 15
	2																	Da
	1																	Da
	0																	Da
14	3	Key A						Access Bits				Key B						Sector Trailer 14
	2																	Da
	1																	Da
	0																	Da
:	:																	
:	:																	
:	:																	
1	3	Key A						Access Bits				Key B						Sector Trailer 1
	2																	Da
	1																	Da
	0																	Da
0	3	Key A						Access Bits				Key B						Sector Trailer 0
	2																	Da
	1																	Da
	0																	Manufacturer Blo

3.6.1 厂商段

厂商段是存储器第一个区的第一个数据段（段 0）。它包含了 IC 卡厂商的数据。基于保密性和系统的

安全性，这一段在 IC 卡厂商编程之后被置为写保护。



3.6.2 数据段

所有的区都包含 3 个段（每段 16 字节）保存数据（区 0 只有两个数据段和一个只读的厂商段）。

数据段可以被以下的访问位（access bits）配置：

- 读 / 写段，用于譬如无线访问控制
- 值段，用于譬如电子钱包，它需要额外的命令，像直接控制保存值的增加和减少

在执行任何存储器操作前都要先执行确认命令。

3.6.2.1 值段

值段可以实现电子钱包的功能。(有效的命令有：读、写、增、减、恢复、发送)。

值段有一个固定的数据格式，可以进行错误检测和纠正并备份管理。

值段只能在值段格式的写操作时产生：

- 值：表示一个带符号 4 字节值。这个值的最低一个字节保存在最低的地址中。取反的字节以标准 2 的格式保存。为了保证数据的正确性和保密性，值被保存了 3 次，两次不取反保存，一次取反保存。
- Adr：表示一个 1 字节地址，当执行强大的备份管理时用于保存存储段的地址。地址字节保存了 4 次，取反和不取反各保存两次。在执行增、减、恢复、传送操作时，地址保持不变。它只能通过写命令改变。

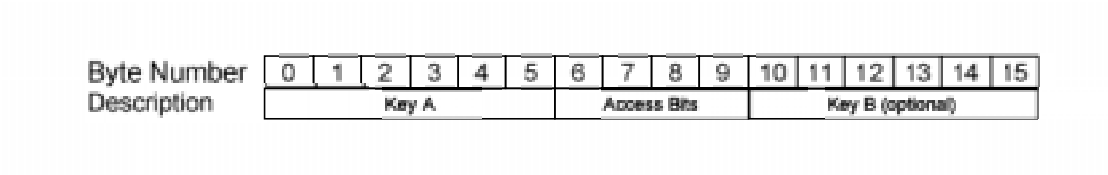
3.6.3 区尾（段 3）

每个区都有一个区尾，它包括：

- 密钥 A 和 B（可选），读密钥时返回逻辑“0”
- 访问这个区中 4 个段的条件（保存在第 6 字节～第 9 字节）。访问位（access bits）也可以指出数据段的类型（读 / 写或值）。

如果不需要密钥 B，那么段 3 的最后 6 字节可以作为数据字节。

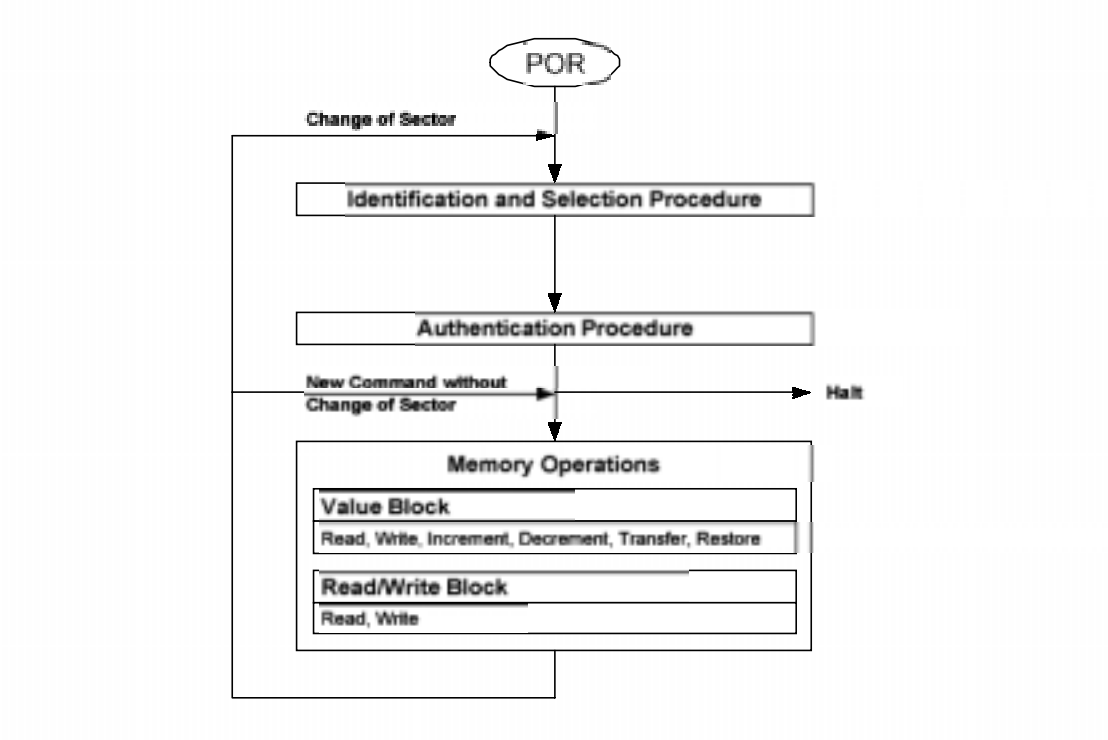
用户数据可以使用区尾的第 9 字节。这个字节具有和字节 6、7 和 8 一样的访问权。



3.7 访问存储器

在执行任何存储器操作以前，卡必须要被选中并经过确认。

编址段可能的存储器操作要根据使用的密钥和保存在相应区尾的访问条件决定。



存储器操作		
操作	描述	有效的段类型
读	读一个存储器段	读 / 写，值和区尾
写	写一个存储器段	读 / 写，值和区尾
增	增加段的内容并将结果保存在内部数据寄存器	值
减	减段的内容并将结果保存在内部数据寄存器	值
传送	将内部数据寄存器的内容写到段中	值
恢复	将段的内容读到内部数据寄存器中	值

3.7.1 访问条件

每个数据段和区尾的访问条件由 3 个位来定义，它们以取反和不取反的形式保存在指定区的区尾中。

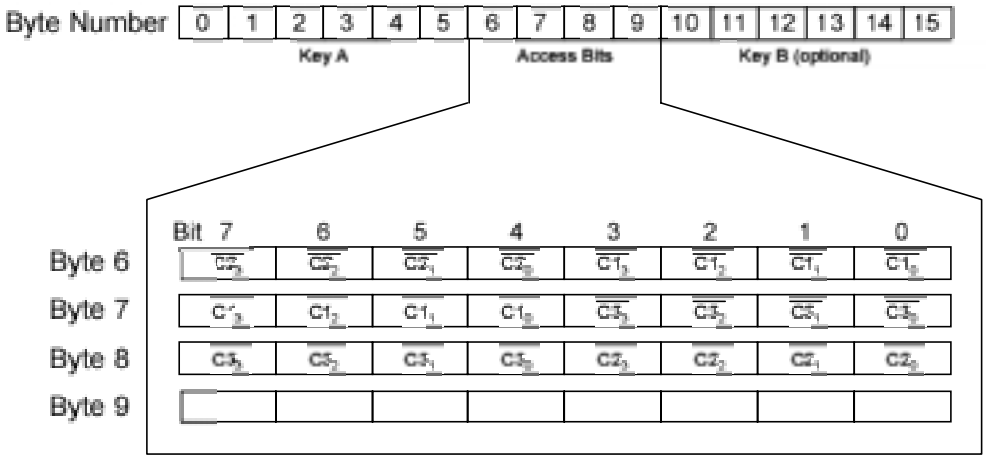
访问位控制了使用密钥 A 和 B 访问存储器的权力。当知道相关的密钥和当前的访问条件时，可以修改访问条件。

注：在下面的描述中，访问位是以不取反的形式显示。

MF1 IC S50 的内部逻辑确保命令只在确认完毕后执行，否则不会执行。

访问位	有效命令		段	描述
$C1_3C2_3C3_3$	读，写	→	3	区尾
$C1_2C2_2C3_2$	读，写，增，减，传送，恢复	→	2	数据段
$C1_1C2_1C3_1$	读，写，增，减，传送，恢复	→	1	数据段
$C1_0C2_0C3_0$	读，写，增，减，传送，恢复	→	0	数据段

注：存储器访问外部逻辑时检查访问条件的格式。如果它检测到格式被破坏，整个区是不可逆的分块。（if it detects a format violation the whole sector is irreversible blocked.）



3.7.2 区尾的访问条件

区尾（段 3）的访问位，密钥和访问位的读写访问可分为“从不”、“密钥 A”、“密钥 B”或“密钥 A|B”（密钥 A 或密钥 B）。

在片给区尾和密钥 A 传送访问条件被预定义为传送配置。由于密钥 B 可以在传输配置中被读出，新的卡要用密钥 A 确认。

由于访问位可以被阻塞，在个人化卡（personalization of cards）的时候要特别注意。（Since the access bits themselves can also be blocked, special care should be taken during personalization of cards.）

访问位			访问条件						注释
			密钥 A		访问位		密钥 B		
C1	C2	C3	读	写	读	写	读	写	
0	0	0	从不	密钥A	密钥 A	从不	密钥A	密钥A	密钥 B 可以被读

0	1	0	从不	从不	密钥 A	从不	密钥A	从不	密钥 B 可以被读
1	0	0	从不	密钥B	密钥 A|B	从不	从不	密钥B	
1	1	0	从不	从不	密钥 A|B	从不	从不	从不	
0	0	1	从不	密钥A	密钥 A	密钥A	密钥A	密钥A	密钥 B 可以被读，传输配置
0	1	1	从不	密钥B	密钥 A|B	密钥B	从不	密钥B	
1	0	1	从不	从不	密钥 A|B	密钥B	从不	从不	
1	1	1	从不	从不	密钥 A|B	从不	从不	从不	

注：用灰色标明的行是密钥 B 可被读的访问条件，此时密钥 B 可以存放数据。

3.7.3 数据段的访问条件

数据段（段 0～2）的访问位，读 / 写访问可分为“从不”、“密钥 A”、“密钥 B”或“密钥 A|B”（密钥 A 或密钥 B）。相关访问位的设置定义了应用以及相应的应用命令。

- 读 / 写段：可以进行读和写操作。
- 值段：可以进行增、减、传送和恢复的值操作。其中一种情况中（“001”）只能对不可再充电的卡进行读和减操作。另一种情况中（“110”）使用密钥 B 可以再充电。
- 厂商段：无论设置任何的访问位这段都是只读！
- 密钥管理：在传输配置中，密钥 A 必须用于确认[1]

访问位			访问条件				应用
C1	C2	C3	读	写	增	减，传送，恢复	
0	0	0	密钥 A|B[1]	密钥 A|B[1]	密钥 A|B[1]	密钥 A|B[1]	传送配置
0	1	0	密钥 A|B[1]	从不	从不	从不	读 / 写段
1	0	0	密钥 A|B[1]	密钥 B[1]	从不	从不	读 / 写段
1	1	0	密钥 A|B[1]	密钥 B[1]	密钥 B[1]	密钥 A|B[1]	值段
0	0	1	密钥 A|B[1]	从不	从不	密钥 A|B[1]	值段
0	1	1	密钥 B[1]	密钥 B[1]	从不	从不	读 / 写段
1	0	1	密钥 B[1]	从不	从不	从不	读 / 写段
1	1	1	从不	从不	从不	从不	读 / 写段

[1] 如果密钥 B 可以在相应的区尾被读出，它就不能用于确认（在前面所有表中的灰色行）。结果：如果 RWD 要用这些（带灰色标记的）访问条件的密钥 B 确认任何段，卡会在确认后拒绝任何存储器访问操作。