ICS 35.040
L 80
备案号:44637—2014

GM

中华人民共和国密码行业标准

GM/T 0035.2—2014

射频识别系统密码应用技术要求
第2部分:电子标签芯片密码应用技术要求

**Specifications of cryptographic application for RFID systems—
Part 2: Specification of cryptographic application for RFID tag chip**

2014-02-13 发布　　2014-02-13 实施

国家密码管理局　　发布

中华人民共和国密码
行业标准
射频识别系统密码应用技术要求
第2部分:电子标签芯片密码应用技术要求
GM/T 0035.2—2014
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)64275323 发行中心:(010)51780235
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 1 字数 24 千字
2014年4月第一版 2014年4月第一次印刷
*
书号:155066·2-27017 定价 18.00 元

GM/T 0035.2-2014

目　　次

前　言

GM/T 0035《射频识别系统密码应用技术要求》分为五个部分：

——第1部分：密码安全保护框架及安全级别；

——第2部分：电子标签芯片密码应用技术要求；

——第3部分：读写器密码应用技术要求；

——第4部分：电子标签与读写器通信密码应用技术要求；

——第5部分：密钥管理技术要求。

本部分为GM/T 0035的第2部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分由密码行业标准化技术委员会提出并归口。

本部分起草单位：上海复旦微电子集团股份有限公司、北京中电华大电子设计有限责任公司、上海华虹集成电路有限责任公司、北京同方微电子有限公司、复旦大学、兴唐通信科技有限公司、上海华申智能卡应用系统有限公司、航天信息股份有限公司、北京华大智宝电子系统有限公司。

本部分主要起草人：俞军、董浩然、周建锁、梁少峰、吴行军、谢文录、王俊宇、柳逊、王俊峰、徐树民、陈跃、顾震、王云松、王会波。

射频识别系统密码应用技术要求
第2部分:电子标签芯片密码应用技术要求

1 范围

GM/T 0035的本部分规定了采用密码技术的电子标签芯片涉及的密码算法、安全认证、数据存储和通信安全的技术要求。附录A给出了一个电子标签芯片示例。

本部分适用于采用密码安全技术的电子标签芯片的设计开发、生产制造和应用。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GM/T 0035.1—2014 射频识别系统密码应用技术要求 第1部分:密码安全保护框架及安全级别

GM/T 0035.4—2014 射频识别系统密码应用技术要求 第4部分:电子标签与读写器通信密码应用技术要求

GM/T 0035.5—2014 射频识别系统密码应用技术要求 第5部分:密钥管理技术要求

3 术语和定义

GM/T 0035.1—2014界定的术语和定义适用于本文件。

4 符号和缩略语

GM/T 0035.1—2014界定的符号和缩略语适用于本文件。

5 密码安全要素

5.1 机密性

5.1.1 存储信息的机密性

电子标签对存储在电子标签内的敏感信息采用密码算法进行加密保护,确保除合法读写器外,其余任何读写器不能获得该数据。

存储信息的机密性保护应采用密码算法加密完成。

采用对称密码算法分组加密方式时,用L_D表示明文数据的长度,在明文数据前加上L_D产生新的数据块,并将该数据块按照密码算法分组长度要求进行分组,如果最后一组数据长度小于密码算法分组长度,则应进行填充补齐。填充方式为在最后一组数据后填充一个字节十六进制'80',如果仍小于密码算法分组长度,则填充'00'至分组长度。在数据分组完成后,采用密码算法和加密密钥对该数据逐组加密后存储。在读取该数据时,对于存储的密文数据,采用同样的密码算法和加密密钥对其进行解密,并

根据明文数据长度 L_D 截取得到完整的明文数据。

5.1.2 传输信息的机密性

电子标签与读写器通信时，电子标签对传输的敏感信息采用密码算法进行加密保护，用于保证该传输数据在被截获后无法得到明文数据，达到数据传输的机密性要求。

传输信息机密性保护须通过对传输的明文数据进行加密完成，采用流加密或分组加密的方式进行。

传输信息机密性的实现过程见 GM/T 0035.4—2014。

5.2 完整性

5.2.1 存储信息的完整性

电子标签采用密码算法对存储在电子标签内的敏感信息进行校验计算，以发现数据被篡改、删除和插入等情况，确保存储数据的完整性。

存储信息完整性保护应采用密码算法，通过对存储的数据加校验码的方式进行。具体方式是在存储数据的同时存储该数据相关的校验码。

采用对称密码算法或密码杂凑函数计算校验码时，实现方式见 GM/T 0035.4—2014 中 7.2.1 和 7.2.2规定的方法。

采用非对称密码算法产生的数字签名可用于数据完整性校验。

5.2.2 传输信息的完整性

电子标签与读写器通信时，电子标签采用密码算法对传输的数据进行校验计算，以发现数据被篡改、删除和插入等情况，达到传输过程中的数据完整性要求。

传输信息的完整性实现方式见 GM/T 0035.4—2014。

5.3 抗抵赖

5.3.1 抗电子标签原发抵赖

抗电子标签原发抵赖是指标签信息的原发者(读写器或第三方)采用密码算法对写入电子标签内的数据进行数字签名操作，确保产生该数字签名的原发者不能成功地否认曾经生成过该数据。

电子标签通过存储标签信息原发者产生的数字签名来实现抗电子标签原发抵赖功能。

5.3.2 抗电子标签抵赖

支持抗电子标签抵赖时，电子标签应具有产生数字签名功能。

5.3.3 抗读写器抵赖

电子标签具有抗读写器抵赖功能时，电子标签应能够对读写器产生的数字签名进行验证，达到抗读写器抵赖的要求。

5.4 身份鉴别

5.4.1 唯一标识符鉴别

唯一标识符鉴别采用与电子标签唯一标识符相关的验证码鉴别方式。

唯一标识符鉴别需要在电子标签中存储 UID 以及验证码(MAC)，该 MAC 是由 UID 与相关应用信息关联后采用密码算法计算产生，并在发行电子标签时写入。

唯一标识符鉴别的实现方式见 GM/T 0035.4—2014。

5.4.2 电子标签对读写器的挑战响应鉴别

电子标签对读写器的挑战响应鉴别的实现方式见 GM/T 0035.4—2014。

5.4.3 读写器对电子标签的挑战响应鉴别

读写器对电子标签的挑战响应鉴别的实现方式见 GM/T 0035.4—2014。

5.5 访问控制

电子标签数据访问控制采用密码算法对数据读写、密钥存储、密钥更新以及数值化数据的增减等操作设置控制权限。对不同的权限应设置不同的密钥进行访问控制，阻止非授权的访问。

在用户应用时，读写器只能按照电子标签发行时所设置的访问控制权限对电子标签进行相关操作。

5.6 审计记录

电子标签对涉及安全的数据及相关操作进行记录并存储，内容至少包括使用主体、使用时间、执行的操作等，用于应用系统审计所记录数据和操作的安全性。

5.7 密码配置

5.7.1 密码算法

电子标签的密码算法配用要求见 GM/T 0035.1—2014。

5.7.2 密钥管理

电子标签密钥管理涉及密钥注入、密钥存储和密钥使用，相关要求见 GM/T 0035.5—2014。

5.8 其他安全措施

电子标签应设计有抗功耗分析、抗电磁分析、抗故障分析、抗物理攻击等安全防护措施，以保护敏感信息的安全。

6 密码安全技术要求

射频识别系统不同安全级别对电子标签芯片密码安全技术的要求不同，电子标签芯片密码安全技术要求应符合表 1 的规定。

表 1 电子标签芯片密码安全技术要求

密码安全要素		射频识别系统密码安全级别			
		1 级	2 级	3 级	4 级
机密性	存储信息的机密性			√	√
	传输信息的机密性			√	√
完整性	存储信息的完整性			√	√
	传输信息的完整性			√	√

表 1（续）

密码安全要素			射频识别系统密码安全级别			
			1 级	2 级	3 级	4 级
抗抵赖	抗电子标签原发抵赖				√	√
	抗电子标签抵赖					√
	抗读写器抵赖					√
身份鉴别	唯一标识符鉴别		√			
	电子标签对读写器的挑战响应鉴别				√	√
	读写器对电子标签的挑战响应鉴别			√	√	√
访问控制				√	√	√
审计记录						√
密码配置	密码算法	对称算法		√	√	√
		非对称算法				√
		密码杂凑函数				√
	密钥管理	密钥注入		√	√	√
		密钥存储		√	√	√
		密钥使用		√	√	√

注 1：“√”表示不同安全级别的射频识别系统中采用的电子标签应具备的密码安全要素。

注 2：表中规定的是射频识别系统各安全级别对电子标签芯片的最低安全要求。

附 录 A
（资料性附录）
电子标签芯片实例

A.1 电子标签分类

A.1.1 标识类

具有可读取的信息，并以此识别出该标签唯一性的电子标签。该类电子标签不具备密码技术保护功能，可用于物流跟踪和物品识别等应用。通常，该类标签适用于安全级别为第一级的射频识别系统。

A.1.2 防伪类

具备标识类电子标签功能，并采用密码技术防止被复制和标签存储信息被篡改等防伪特性的电子标签，可用于电子门票和物品防伪等应用。通常，该类标签适用于安全级别为第二级的射频识别系统。

A.1.3 证件、小额支付类

具备防伪类电子标签基本安全功能，并具有存储信息的机密性和完整性、传输信息的机密性和完整性的电子标签，可用于电子证件和小额支付等应用。通常，该类标签适用于安全级别为第三级的射频识别系统。

A.1.4 其他类

不属于上述三种类型的其他种类电子标签。

A.2 防伪类电子标签芯片实例

本芯片为支持国产密码算法的电子标签芯片，适用于安全级别为第二级的射频识别系统，可用作防伪类电子标签。

a) 功能特性

工作频率：13.56 MHz

通讯速率：106 kbit/s

工作距离：0～10 cm(与读写器相关)

数据通信完整性：数据帧 16 位 CRC，数据字节奇偶校验，位编码，位记数

存储器容量：1024×8 bit EEPROM

通讯协议：ISO 14443 Type A

b) 安全特性

支持国产密码算法 SM7

双向身份鉴别

c) 功能框图

芯片整体功能如图 A.1 所示。

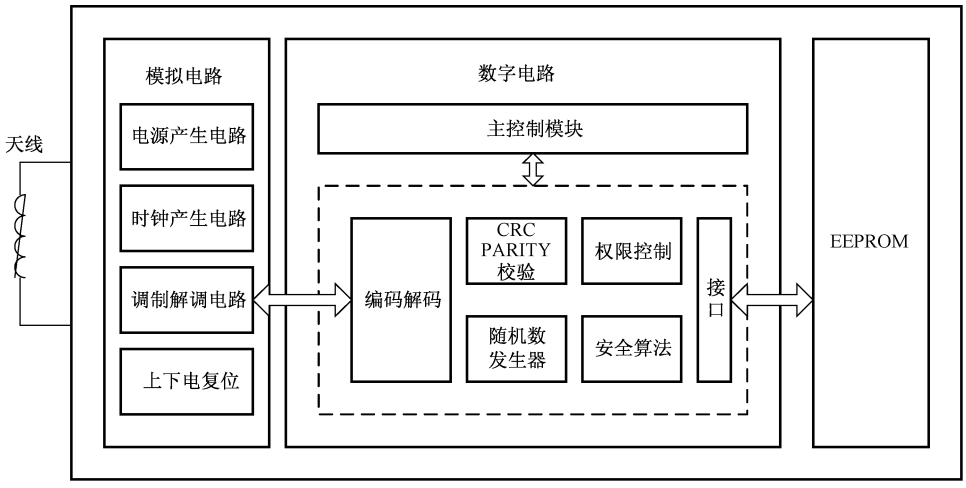

图 A.1　功能框图

A.3　数据存储结构

存储器为 1 KB,分为存储区 A 和存储区 B。每个存储区大小为 512 字节,每个存储区分为 32 个块,每个块为 16 字节。块定义如图 A.2。

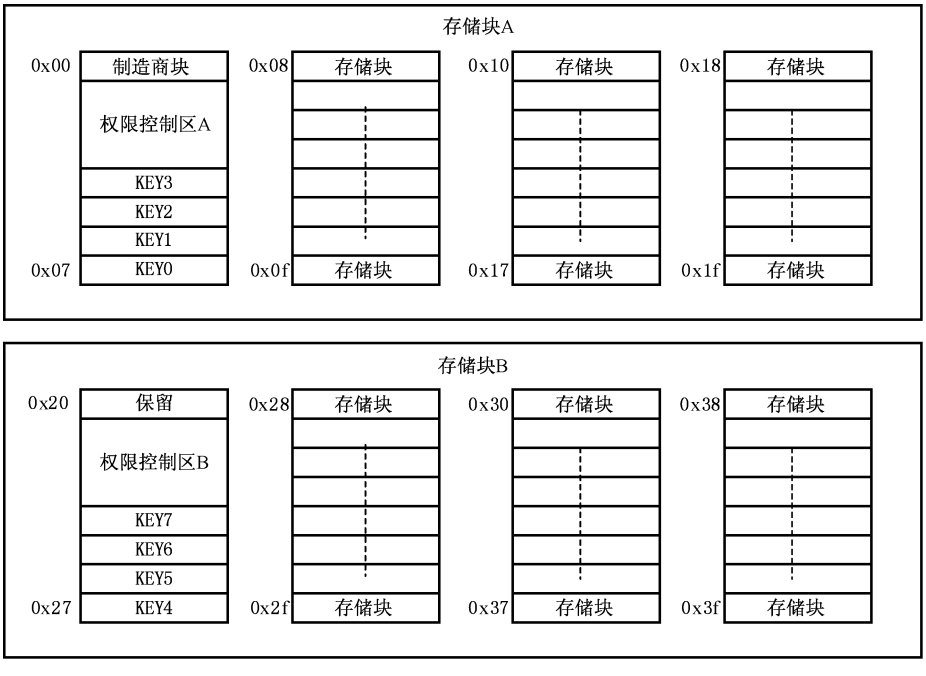

图 A.2　存储区

A.4　唯一标识符说明

制造商块地址是 0x00,如表 A.1 所示。它包含 IC 制造商信息、唯一标识符(UID)。由于安全和系统需要,当 IC 制造商在生产过程中编程以后,这个块是写保护的,即不可改写,符合本部分中对电子标

签唯一标识符的要求。

表 A.1　制造商块字节编码(地址:0x00h)

字节	0	1	2	3	4	5～15
内容	唯一标识符(UID)				BCC	制造商信息

其中,BCC 为唯一标识符(UID)校验字节,Byte4 = Byte0 ^ Byte1 ^ Byte2 ^ Byte3。

A.5　数据访问控制权限说明

权限区 A 的块地址从 0x01h～0x03h,占用 3 个存储块。字节 A0～A23 分别对应存储块 0x08h～0x1fh 共 24 块的控制权限。权限区 B 的块地址从 0x21h～0x23h,占用 3 个存储块。字节 A24～A47 分别对应存储块 0x28h～0x3fh 共 24 块的控制权限如表 A.2～表 A.7 所示。

表 A.2　数据访问控制权限 A(地址:0x01h)

字节	0	1	2	3	4	5	6	7
内容	A0	/A0	A1	/A1	A2	/A2	A3	/A3
字节	8	9	10	11	12	13	14	15
内容	A4	/A4	A5	/A5	A6	/A6	A7	/A7

表 A.3　数据访问控制权限 A(地址:0x02h)

字节	0	1	2	3	4	5	6	7
内容	A8	/A8	A9	/A9	A10	/A10	A11	/A11
字节	8	9	10	11	12	13	14	15
内容	A12	/A12	A13	/A13	A14	/A14	A15	/A15

表 A.4　数据访问控制权限 A(地址:0x03h)

字节	0	1	2	3	4	5	6	7
内容	A16	/A16	A17	/A17	A18	/A18	A19	/A19
字节	8	9	10	11	12	13	14	15
内容	A20	/A20	A21	/A21	A22	/A22	A23	/A23

表 A.5　数据访问控制权限 B(地址:0x21h)

字节	0	1	2	3	4	5	6	7
内容	A24	/A24	A25	/A25	A26	/A26	A27	/A27
字节	8	9	10	11	12	13	14	15
内容	A28	/A28	A29	/A29	A30	/A30	A31	/A31

表 A.6　数据访问控制权限 B(地址:0x22h)

字节	0	1	2	3	4	5	6	7
内容	A32	/A32	A33	/A33	A34	/A34	A35	/A35
字节	8	9	10	11	12	13	14	15
内容	A36	/A36	A37	/A37	A38	/A38	A39	/A39

表 A.7　数据访问控制权限 B(地址:0x23h)

字节	0	1	2	3	4	5	6	7
内容	A40	/A40	A41	/A41	A42	/A42	A43	/A43
字节	8	9	10	11	12	13	14	15
内容	A44	/A44	A45	/A45	A46	/A46	A47	/A47

每个存储块的权限由 1 个字节组成(另外 1 个字节对其取反后作为备份)。b7 位的设置决定数据块 的数据类型;b5、b6 决定采用哪个密钥作为该数据块的读操作(或减值操作)访问密钥;b3、b4 决定采用哪个密钥作为该数据块的写操作(或加/减值操作)访问密钥;b2 作为校验位,为 b7～b3 的异或;b1 是 b2 的取反; b0 是密钥区选择位。如表 A.8 所示。

表 A.8　权限控制字节定义

位	说明
b7	0:数据 1:数值
b[6:5]	数据型:读密钥地址 数值型:读/减值/存储/传输密钥地址 00:key0 或 key4 01:key1 或 key5 10:key2 或 key6 11:key3 或 key7
b[4:3]	数据型:读/写密钥地址 数值型:读/加/减值/存储/传输密钥地址 00:key0 或 key4 01:key1 或 key5 10:key2 或 key6 11:key3 或 key7
b2	校验位,b7～b3 的异或
b1	校验位,b2 取反
b0	密钥区选择位 0:选取 A 区密钥 key0～key3 1:选取 B 区密钥 key4～key7

注 1: b2 = b3⊕b4⊕b5⊕b6⊕b7　b1=/b2

注 2: 制造商块只有读权限。

注 3: key0 为主控密钥,只有通过 key0 进行身份鉴别通过后才能对密钥区与权限区执行写操作。

A.6 密码算法说明

电子标签采用 SM7 密码算法，用于电子标签和读写器的双向鉴别和数据通信中的加解密操作。

A.7 身份鉴别和数据通信加密说明

电子标签采用 GM/T 0035.4—2014 规定的双向身份鉴别和用分组密码算法的密钥协商，并对过程进行适当合并。

A.7.1 双向身份鉴别

芯片被读写器选中后(REQA、ANTI、SELECT)，必须进行双向身份鉴别，通过鉴别后，才能对鉴别密钥对应的块进行相应控制权限的访问。鉴别的技术要求如下：

——电子标签和读写器采用 SM7 国产密码算法。

——电子标签和读写器使用相同的密钥 KEY。

——电子标签和读写器分别使用各自的随机数发生器。

鉴别过程具体流程如下(见图 A.3)：

a) 读写器发送鉴别指令以及指令参数(密钥块地址)。

b) 电子标签接收指令后发送由随机数发生器产生的 32 位 Rb。

c) 读写器收到 Rb 后，由随机数发生器产生 32 位随机数 Ra，并以 128 位 KEY 为密钥进行加密，加密的明文为 Ra(左半部分)和 Rb(右半部分)。加密结束，发送 64 位密文 Token1 (低位先发)。

d) 电子标签接收到 Token1 之后对其进行解密，解密后得到的明文右半部分 Rb′与之前产生的 Rb 比较。

e) 电子标签比较 Rb′正确后，加密生成 Token2，加密的明文为电子标签新产生的 32 位随机数 Rb″(左半部分，Rb″用于密钥协商)和解密 Token1 得到的 Ra′(右半部分)，得到的 64 位密文为 Token2。如果 Rb′与 Rb 不同，则电子标签无响应并返回到空闲/挂起状态。

f) 电子标签加密完成后，发送 Token2(低位先发)。在发送完信息后，电子标签等待读写器发送的后续命令。

g) 读写器接收到 Token2 后，解密并比较所得到的 Ra′与原先发送的 Ra，如果 Ra′比较正确，鉴别通过，否则鉴别失败。

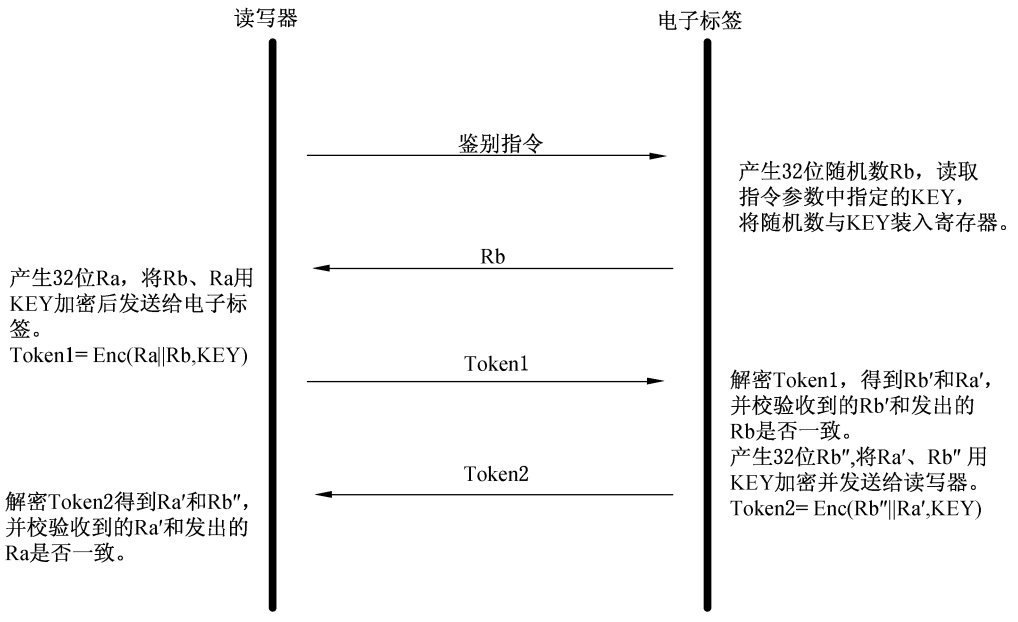

图 A.3　鉴别流程

鉴别指令通过参数选择 key0～key7 进行认证。某一密钥的鉴别通过后，所有该密钥对应的访问权限全部打开。

A.7.2　通信数据的加密传输

对通信数据的加密采用基于 SM7 算法的流加密方式，数据发送端通过 OFB 模式循环产生密码流，并将通信明文数据与密码流异或后发出；数据接收端通过相同方法产生相同的密码流，将接收到的加密数据与密码流异或后得到数据明文。

在图 A.3 描述的双向身份鉴别过程结束后，电子标签与读写器都继续使用当次身份鉴别过程所使用的密钥 KEY，将身份鉴别过程中产生的 Token2 作为初始向量，通过 SM7 算法的 OFB 模式运算，所产生的加密结果用作流加密的密码流，与通信数据明文（密文）异或后得到通信数据密文（明文）。

A.8　密钥管理

A.8.1　密钥注入

电子标签芯片中的密钥在电子标签初始化过程中注入。密钥注入完成后，通过使用注入的密钥进行身份鉴别来确认注入的密钥是否正确。

A.8.2　密钥存储

密钥存储在芯片密钥区，密钥区信息任何时候都不能被读出。key0 为主控密钥，只有通过 key0 进行身份鉴别通过后才能对密钥区执行写操作。

A.8.3　密钥使用

密钥用于身份鉴别与访问控制。使用任何一个密钥进行身份鉴别通过后，读写器可以获得与该密钥权限相对应的存储块的访问权限。

A.9 全部指令集说明

电子标签芯片的指令集如表 A.9 所示。

表 A.9 电子标签芯片指令集

指令名称	指令代码(16 进制)	说　明
request std	26	复位应答指令 寻找未被置成暂停状态的电子标签
request all	52	复位应答指令 寻找所有在操作区域内的电子标签
Anti-collision	93	防冲突指令 如果操作区域内有一张或多张电子标签,本指令将用来从这些电子标签中选出一张电子标签
Select Tag	93	选择电子标签指令 在防冲突指令后建立起与选中电子标签的通讯
Authentication	70	身份鉴别指令 鉴别电子标签和读写器的合法性
Read	30	读块指令 读出电子标签中某一块的 16 个字节
Write	A0	写块指令 将数据写入电子标签中的某一块
Increment	C1	加法指令 将电子标签中的数值块加上某一数值,并把结果存于电子标签内的寄存器
Decrement	C0	减法指令 将卡中的数值块减去某一数值并把结果存于电子标签内的寄存器
Restore	C2	存储指令 将电子标签内数值块的内容读到电子标签内的寄存器
Transfer	B0	传输指令 将电子标签内寄存器中的内容写入块中
Halt	50	挂起指令 将电子标签置于暂停状态