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

GM/T 0035.2—2014

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





## 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<br>寻找未被置成暂停状态的电子标签 |
| request all | 52 | 复位应答指令<br>寻找所有在操作区域内的电子标签 |
| Anti-collision | 93 | 防冲突指令<br>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<br>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<br>鉴别电子标签和读写器的合法性 |
| Read | 30 | 读块指令<br>读出电子标签中某一块的 16 个字节 |
| Write | A0 | 写块指令<br>将数据写入电子标签中的某一块 |
| Increment | C1 | 加法指令<br>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<br>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<br>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<br>将电子标签内寄存器中的内容写入块中 |
| Halt | 50 | 挂起指令<br>将电子标签置于暂停状态 |

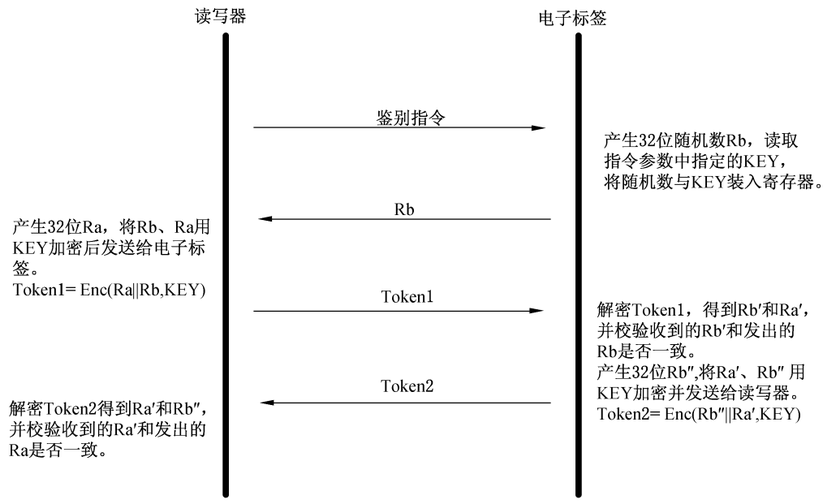


**图 A.3　鉴别流程**

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。





# 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。