

NFC & MIFARE & ISO14443A&B & ISO7816 & ISO15693 & ISO18000 非接触式 IC 卡读写模块

JMY600 系列读写卡模块

ISO18000-3 MODE 3 电子标签操作指南

(Revision 1.04)

北京金木雨电子有限公司

2020/7/22

在使用本产品前请详细阅读本说明书，如果有任何疑问，请联系我们，我们会给您详尽的解答



目录

1	概述.....	2
2	主要性能指标.....	2
3	卡片功能.....	2
4	存储结构.....	3
5	卡片操作.....	3
5.1	说明.....	3
5.2	单标签操作.....	3
5.3	多标签操作.....	5
5.3.1	多标签中寻单标签并操作.....	5
5.3.2	多标签同时操作.....	5



1 概述

本文详细介绍了使用 JMY600 系列读卡模块操作 ISO18000-3 MODE 3 电子标签的操作方法和顺序以及基本卡片功能设计，您可以通过阅读本手册很快速地掌握 ISO18000-3 MODE 3 电子标签的使用。本手册的使用对象为使用 JMY600 系列 RFID 模块的程序员，我们也有通讯协议的例子代码，可以在金木雨的网站上找到。如果在编写程序中依然有任何的问题，请随时联系我们的技术支持，或发送电子邮件到：jinmuyu@vip.sina.com 我们会给您满意的答复。

2 主要性能指标

- 标签价格低廉
- 多种容量的用户存储
- 标签存储空间可以权限设定
- 96 位标签标识符(TID)，包括 48 位唯一序列号
- 具有防冲突机制，支持多卡操作
- 数据保存期为 10 年，可改写 10 万次，读无限次
- 工作温度：-20℃~50℃(湿度为 90%)
- 工作频率：13.56MHZ
- 通信速率：106Kbit/s
- 读写距离：大功率专用读写器：最大 1.5 米；在 JMY600 系列上大于 10 cm

3 卡片功能

ISO18000-3 mode 3 电子标签设计之处是用于物流管理，文档追踪，洗衣自动化，赌场筹码等场景，96 字节 TID，可用范围非常庞大。标签封装形式多样，且价格低廉。

标签优势：灵敏度高，读取距离远，具有先进的防干扰功能，识别速度最高（up to 800tags/s），并且具有可靠而强大的 RFID 技术，适合在噪声和密集标签环境下使用。



4 存储结构

卡片存储结构分为 4 个 Bank (Reserved Memory, UII Memory, TID Memory, User Memory)。每个 Bank 由块组成, 块存储大小为 16bits。详见下表。

Bank 编号	Bank 名称	地址	说明
11 _b	User		
		00h~0Fh	Word 0 of Block 0
10 _b	TID		
		10h~1Fh	TID[15:0]
		00h~0Fh	TID[31:16]
01 _b	UII		
		220h~22Fh	Optional XPC_W2[15:0]
		210h~21Fh	Mandatory XPC_W1[15:0]
			
			UII[15:0]
			
		20h~2Fh	UII[N:N-15]
		10h~1Fh	StoredPC[15:0]
		00h~0Fh	StoredCRC-16[15:0]
00 _b	RESERVED		
		30h~3Fh	Access Passwd[15:0]
		20h~2Fh	Access Passwd[31:16]
		10h~1Fh	Kill Passwd[15:0]
		00h~0Fh	Kill Passwd[31:16]

注：不同厂家标签可能对存储结构中 Bank 的大小和定义做不同规定。

5 卡片操作

5.1 说明

本文的实验卡片型号为 NXP 公司的 ICODE ILT, 型号为: 2L2S1402, 同系列产品还有 2L2S1502 和 2L2S1602, 都可以用来实验。如需厂方的 Datasheet 或样卡, 请与我们的销售人员联系。

5.2 单标签操作

取一张出厂默认格式的新卡放到天线上, 使用 TransPost 软件做这些实验, 请按照顺序发送



如下命令：

- **Inventory:**
寻卡操作，获取卡片 handle，后续指令需填充 handle。注意每次获取的值都不同。
TransPort 中输入：85 00
实际端口发出指令：00 05 00 85 00 80
实际端口收到：00 07 01 85 00 04 57 D0
- **读密钥:**
读取卡片密钥，地址：00h Bank 的 00h 地址开始的 04h（Word 型 16bits）长度
TransPort 中输入：85 02 00 00 00 04 04 57
实际端口发出指令：00 0B 00 85 02 00 00 00 04 04 57 DB
实际端口收到：00 0F 01 85 02 00 00 00 00 00 00 00 04 57 DA
- **写 ACCESS 密钥:**
写卡片 ACCESS 密钥，地址：00h Bank 的 02h 地址开始的 02h 长度的密钥
TransPort 中输入：85 07 00 00 02 02 11 22 33 44 04 57
实际端口发出指令：00 0F 00 85 07 00 00 02 02 11 22 33 44 04 57 9A
实际端口收到：00 07 01 85 07 04 57 D7
- **读密钥:**
读取卡片密钥，地址：00h Bank 的 00h 地址开始的 04h（Word 型 16bits）长度
TransPort 中输入：85 02 00 00 00 04 04 57
实际端口发出指令：00 0B 00 85 02 00 00 00 04 04 57 DB
实际端口收到：00 0F 01 85 02 00 00 00 00 11 22 33 44 04 57 9E
- **设定 ACCESS 密钥读写权限:**
TransPort 中输入：85 05 30 00 20 00 04 57
实际端口发出指令：00 0B 00 85 05 30 00 20 00 04 57 C8
实际端口收到：00 07 01 85 05 04 57 D5
设定后，ACCESS 密钥需要认证后才能读写。
- **标签重新上电**
- **Inventory:**
首先进行寻卡操作。
TransPort 中输入：85 00
实际端口发出指令：00 05 00 85 00 80
实际端口收到：00 07 01 85 00 EA 3B 52
- **读密钥:**
读取卡片密钥，地址：00h Bank 的 00h 地址开始的 04h（Word 型 16bits）长度
TransPort 中输入：85 02 00 00 00 04 EA 3B
实际端口发出指令：00 0B 00 85 02 00 00 00 04 EA 3B 59
实际端口收到：00 08 01 7A 02 04 EA 3B A4（04：表示 Memory locked）



- 认证权限：
DSFID 在 Get system information 命令中从卡片获得。
TransPort 中输入：85 06 11 22 33 44 EA 3B
实际端口发出指令：00 0B 00 85 06 11 22 33 44 EA 3B 1D
实际端口收到：00 07 01 85 06 EA 3B 54
- 读密钥：
读取卡片密钥，地址：00h Bank 的 00h 地址开始的 04h（Word 型 16bits）长度
TransPort 中输入：85 02 00 00 00 04 EA 3B
实际端口发出指令：00 0B 00 85 02 00 00 00 04 EA 3B 59
实际端口收到：00 0F 01 85 02 00 00 00 00 11 22 33 44 EA 3B 1C
- 取消 ACCESS 密钥读写权限：
TransPort 中输入：85 05 30 00 00 00 EA 3B
实际端口发出指令：00 0B 00 85 05 30 00 00 00 EA 3B 6A
实际端口收到：00 07 01 85 05 EA 3B 57
- 恢复密钥：
TransPort 中输入：85 07 00 00 02 02 00 00 00 00 EA 3B
实际端口发出指令：00 0F 00 85 07 00 00 02 02 00 00 00 00 EA 3B 5C
实际端口收到：00 07 01 85 07 EA 3B 55

5.3 多标签操作

取多张出厂默认格式的新卡放到天线上，使用 TransPost 软件做测试，请按照顺序发送如下命令：

5.3.1 多标签中寻单标签并操作

TransPort 中输入：85 01 01
实际端口发出指令：00 06 00 85 01 01 83
实际端口收到：00 07 01 85 01 6F 74 99

之后的测试就可以按照 5.1 节进行测试

5.3.2 多标签同时操作

- 获取所有标签的 TID：
注：该指令执行之后，标签需要重新上电，才能再次执行该指令。
TransPort 中输入：85 0A 02



实际端口发出指令：00 06 00 85 0A 02 8B

实际端口收到：00 3A 01 85 0A 04 0C 0C 0C 0C 00 00 00 00 00 00 40 00 FA B1 58 92 00
00 00 00 00 00 40 00 FA B1 D0 88 00 00 00 00 00 00 40 00 FA B1 F5 23 00 00 00 00 00 40
00 FA B1 4C AB 13

(示例说明：寻到 4 张标签，标签的 TID 长度为 0C 0C 0C 0C h，第一标签信息 00 00 00
00 00 00 40 00 FA B1 58 92……)

- 获取第一张标签的 Handle

TransPort 中输入：85 0B 0C 00 00 00 00 00 00 40 00 FA B1 58 92

实际端口发出指令：00 12 00 85 0B 0C 00 00 00 00 00 00 40 00 FA B1 58 92 51

实际端口收到：00 07 01 85 0B E0 E0 88

之后可以按照 5.1 章节进行测试。

- 获取第二张标签的 Handle

TransPort 中输入：85 0B 0C 00 00 00 00 00 00 40 00 FA B1 D0 88

实际端口发出指令：00 12 00 85 0B 0C 00 00 00 00 00 00 40 00 FA B1 D0 88 C3

实际端口收到：00 07 01 85 0B D5 2F 72

之后可以按照 5.1 章节进行测试。

- 获取第三张标签的 Handle

TransPort 中输入：85 0B 0C 00 00 00 00 00 00 40 00 FA B1 F5 23

实际端口发出指令：00 12 00 85 0B 0C 00 00 00 00 00 00 40 00 FA B1 F5 23 4D

实际端口收到：00 07 01 85 0B 9C 0F 1B

之后可以按照 5.1 章节进行测试。

- 获取第四张标签的 Handle

TransPort 中输入：85 0B 0C 00 00 00 00 00 00 40 00 FA B1 4C AB

实际端口发出指令：00 12 00 85 0B 0C 00 00 00 00 00 00 40 00 FA B1 4C AB 7C

实际端口收到：00 07 01 85 0B 12 3A A0

之后可以按照 5.1 章节进行测试。

注：切换标签进行操作时，必须要根据 TID 重新获取 Handle。