特别说明

AN03005

手持机对ISO14443-4和ISO7816-4标准支持及接口介绍

作者：技术支持部 胡永健

一、 介绍：

IC卡 (Integrated Circuit Card)的发明和发展吸引了世界众多厂商的参与，在这期间涌现了大量新技术和应用。国际标准化组织 (ISO)为 IC卡及相关设备制订了大量的标准，其中包括：

1 接触式 IC卡国际标准

(a) ISO/IEC7816—1 ： 接触式 IC卡的物理特性；

(b) ISO/IEC7816—2 ： 接触式 IC卡的触点尺寸和位置；

(c) ISO/IEC7816—3 ： 接触式 IC卡 (异步卡)的电信号和传输协议 (T=0/T=1),适用于 CPU卡；

(d) ISO/IEC7816—10 ： 接触式 IC卡 (同步卡)的电信号和复位应答，适用于存储卡和加密卡。

2 非接触式 IC卡标准

(a) ISO/IEC14443—1 ： 非接触式 IC卡的物理特性；

(b) ISO/IEC14443—2 ： 非接触式 IC卡的射频能量和信号接口；

(c) ISO/IEC14443—3 ： 非接触式 IC卡的初始化和防冲突 (Type A/Type B)；

(d) ISO/IEC14443—4 ： 非接触式 IC卡的选择应答和传送协议 (T=CL)。

3 传输层及应用层标准

(a) ISO/IEC7816—4 ： 行业间交换用命令；

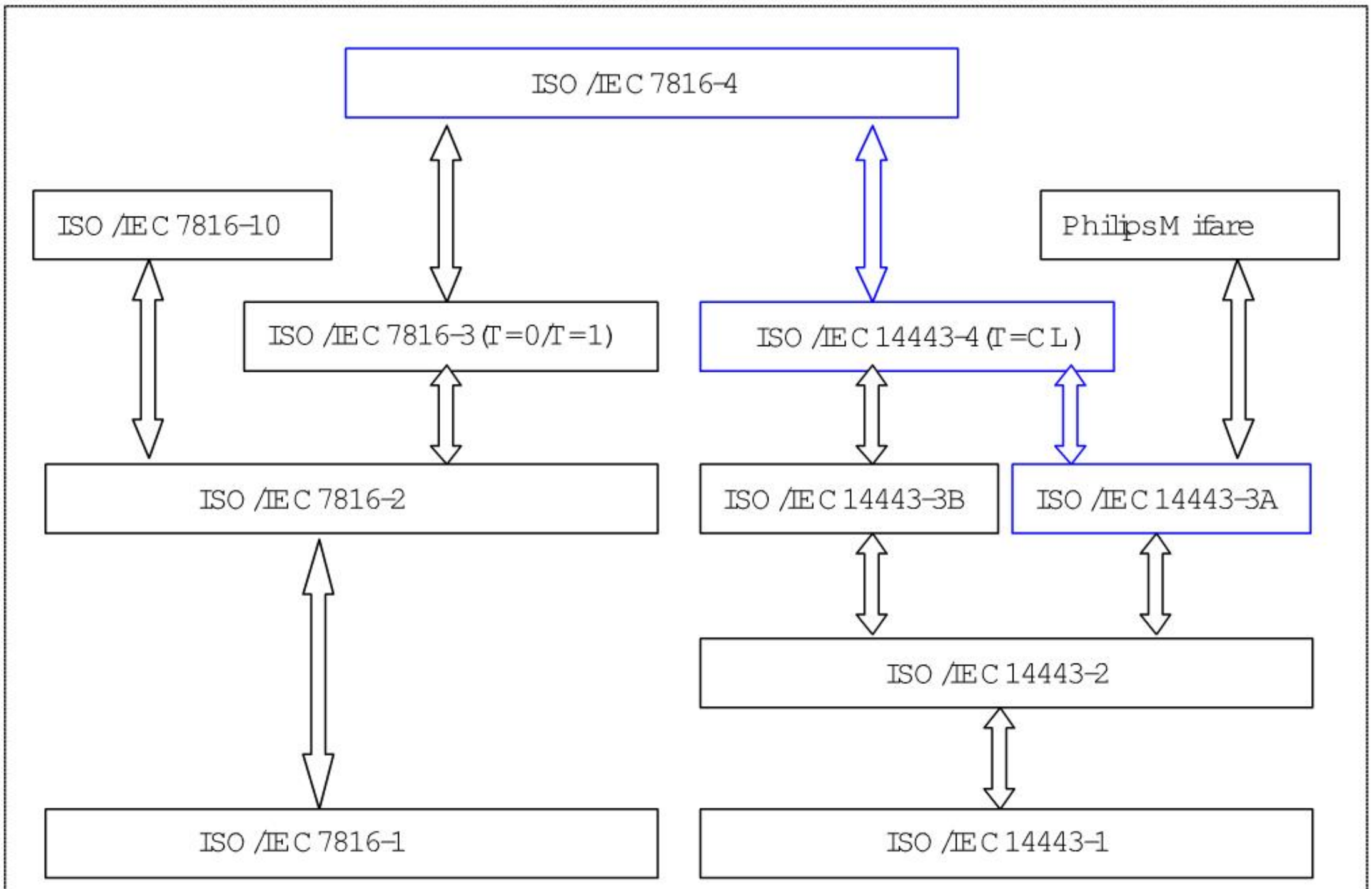
(b) ISO/IEC7816—5 ： 应用标识符的编号系统和注册过程；

(c) ISO/IEC7816—6 ： 行业间数据元；

(e) ISO/IEC7816—7 ： 结构化卡查询语言的行业间命令；

(f) ISO/IEC7816—8 ： 安全有关行业间命令。

在 IC卡相关标准制订过程中遵循了国际标准化组织的开放系统互连模型 (OSI—Open System Interconnection model),各标准之间也相应地存在层次依附关系，见（图 1—1)：



（图 1-1）

现在市场上应用广泛的 Mifare 系列非接触卡都遵循 ISO/IEC14443-1、 ISO/IEC14443-2、ISO/IEC144443-3 Type A标准；此外，新出现的 Mifare DESfire与 Mifare Pro非接触卡还遵循 14443-4 (T=CL)协议标准，见（图 1-2）：

	Mifare Ultra Light	Mifare Standard (1K)	Mifare Standard (4K)	Mifare DESfire	Mifare Pro X
ISO14443-4 Transmission Protocol	NO	NO	NO	YES	YES
ISO14443-3 Initialization & Anticollision	YES	YES	YES	YES	YES
ISO14443-2 RF-Power and Signal Interface	YES	YES	YES	YES	YES
ISO14443-1 Physical Characteristics	YES	YES	YES	YES	YES

（图 1-2）

MifarePro非接触卡是世界上最早出现的真正的双界面 CPU卡，它集 CPU卡与非接触卡优点于一身，并兼具接触式卡接口，它的出现标志着 IC卡技术达到一个新的高度。 本文正是向大家介绍手持机对 Mifare Pro卡的支持能力，也就是提供对 ISO/IEC14443-3 Type A标准、ISO/IEC14443-4(T=CL)标准和 ISO/IEC7816-4标准的支持。

另外，在实际编程操作之前需要一些准备工作：

⑴ 将 mifare530.a和 mifare.a拷贝至系统库文件路径下；

⑵ 将 mifare530.h 、 TPDU_Layer(14443-4).H 、 APDU_Layer(7816-4).H 以及 Industry_Command.H头文件拷贝至系统包含文件路径下；

⑶ 需改 LD文件为：GROUP(-lgcc -lg -lm -lm2002 -lmcard -lconso -lstd mifare530.a mifare.a)。

二、 标准支持及接口介绍

前面提到， IC卡相关标准的制订遵循 ISO/OSI参考模型，手持机等 IC卡读写设备必须实现与 IC卡相对应的标准协议层才能与 IC卡进行通信；也就是说，若要实现对 MifarePro卡的支持，手持机需提供对 ISO14443-1、ISO1443-2、ISO14443-3A、ISO14443-4、ISO7816-4标准以及更上层应用协议的支持。

1 对 ISO14443-1与 ISO14443-2标准的支持

ISO14443-1标准规定了非接触式 IC卡的物理特性； ISO14443-2标准针对非接触式 IC卡的射频能量和信号接口进行标准化。

手持机 Mifare扩展板使用了 Mifare RC531集成芯片，通过它手持机可实现对 ISO14443-1、ISO14443-2以至于 ISO14443-3A标准的支持。

2 对 ISO14443-3 Type A标准的支持

ISO14443-3标准规定了非接触式 IC卡的初始化和防冲突过程，其中又分为 TypeA标准和 Type B标准。Mifare RC531同时支持 Type A和 Type B标准。在≪MC2002 Hand-Held Smart Card Read/Write Device (RWD) Optional Device Library Manual: MIFARE® Accessing Library≫中提供了 Mifare RC531的接口控制 API以及支持 ISO14443-3A标准的 API接口。

⑴ Mifare扩展板接口控制 API:

a. 接口上电初始化： InitMC530();

b. 接口断电： MC530off();

⑵ 支持 ISO14443-3A标准的 API接口

a. 登记 (Polling)与唤醒 (WAKE-UP)： CardTypeARequest();

b. 防碰撞 (Anticollision)： CardTypeAAnticoll();
CardTypeAAnticollLevel1();

c. 选卡 (Selection)： CardTypeASelect();
CardTypeASelectLevel1();

d. 停止状态 (HALT)： CardTypeAHalt();

有关这些 API的详细使用方法请查阅相关文档，这里就不再赘述。

3 对 ISO14443-4标准的支持

ISO14443-4主要是对非接触式 IC卡的选择应答、传送协议 (T=CL)等卡操作过程进行标准化。

ISO14443-4标准的 T=CL传送协议是类似于 ISO7816-3标准 T=1协议的链路层协议，主要功能是进行读写设备与 Mifare卡之间的链路维护；另外， ISO14443-4还规定了 TypeA 类卡的激活序列，见图 2-1)：

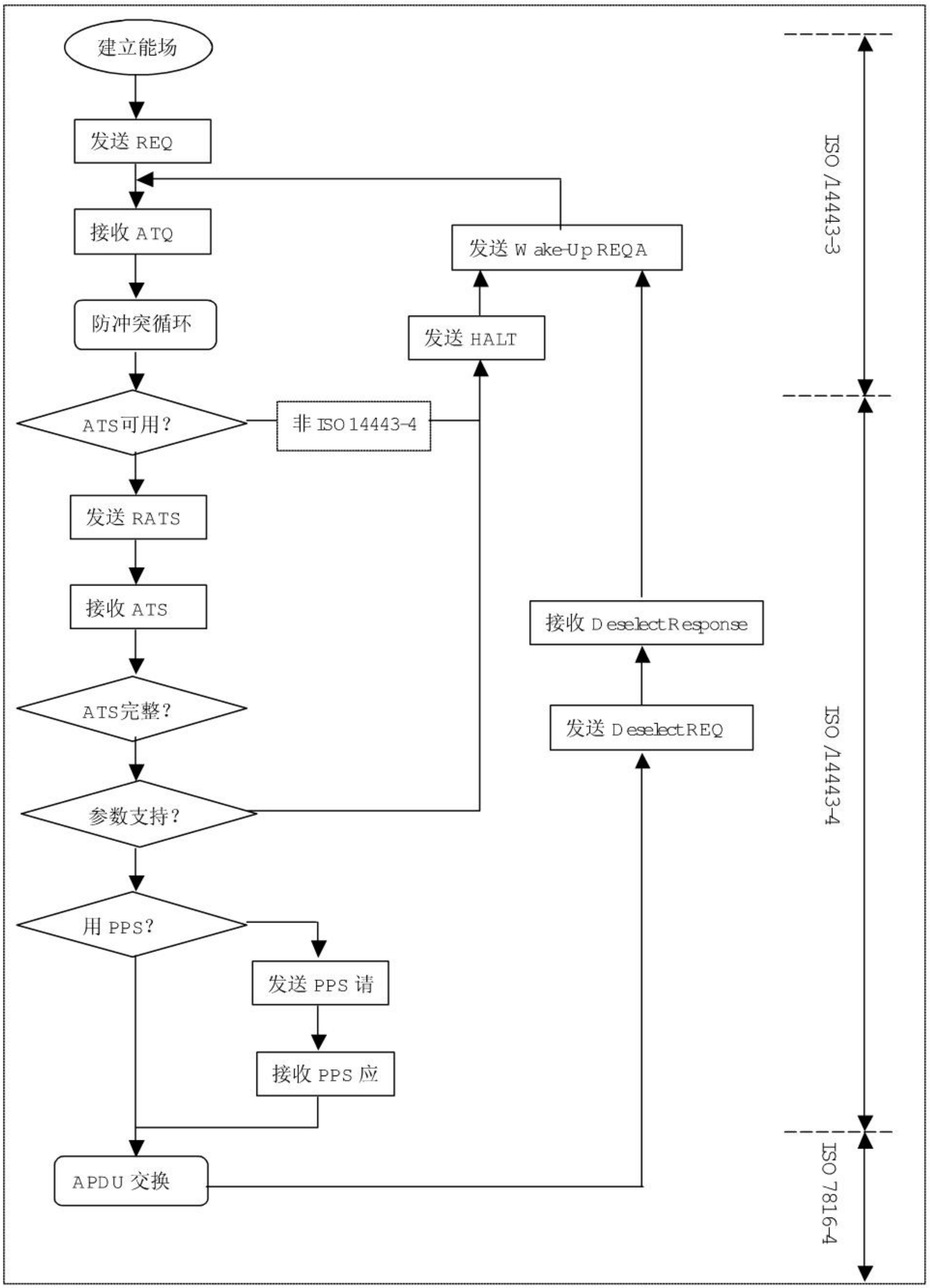


图 2-1)

从图中可知读写设备与 MifarePro卡链路层 (ISO14443-4规定)处理包含四部分：RATS (Request for Answer To Select)请求及应答、协议和参数选择 (PPS—Protocol and Parameter Selection)、TPDU (Transport Protocol Data Unit)交换以及解除激活序列 (Deselect)。在协议实现中我们对除PPS之外的其它三部分进行封装，并提供相应的 API接口。

(1) extern char CardTypeARATS (unsigned char CID, unsigned char ATS[], unsigned short *ATS_Length);

功用：由手持机向卡发送 RATS 并等待 ATS (Answer To Select)应答。

参数： unsigned char CID—由读写设备给非接触卡指定的 ID号 (0x00-0x0F)，用于多卡启动。不使用此功能可将参数置为 NoUsing

unsigned char ATS[]—用于存储返回的 ATS;

unsigned short *ATS_Length—用于返回 ATS长度。

返回值： a. 正确执行，返回 MI_OK;

b. ISO14443-3A及其以下级别的错误 定义在 Mifare530.h中);

c. ISO14443-4级别错误 定义在 TPDU_Layer (14443-4).h中)：

MI_TPDU_CRC_ERROR————TPDU层校验错;

MI_TPDU_EXCHANGE_ERROR——TPDU层帧交换错。

(2) extern char CardTypeADeselect (unsigned char CID);

功用：由手持机向卡发送 Deselect请求，并等待确认应答;

参数： unsigned char CID——由读写设备给非接触卡指定的 ID号 (0x00-0x0F)，用于区分处于活动状态 (Active State)的不同的 Mifare卡。不使用此功能可将参数置为 NoUsing

返回值： a. 正确执行，返回 MI_OK;

b. ISO14443-3A及其以下级别的错误 定义在 Mifare530.h中);

c. ISO14443-4级别错误 定义在 TPDU_Layer (14443-4).h中)：

MI_TPDU_CRC_ERROR————TPDU层校验错;

MI_TPDU_EXCHANGE_ERROR——TPDU层帧交换错。

(3) extern char CardTypeALinkLayerExchange (unsigned char CID, unsigned char NAD, unsigned char APDU_Data[], unsigned short APDU_Data_Length, unsigned char Rec_APDU[], unsigned short *Rec_APDU_Length);

功用：由手持机向 Mifare卡发送 TPDU 并等待应答 TPDU此 API由上层协议使用，用户不需直接调用)。

参数： 略;

返回值：同上。

4 对 ISO7816-4标准的支持

ISO7816-4 主要针对 CPU卡的数据结构、安全信息、应用协议数据单元 (APDU—Application Protocol Data Unit)的信息结构、行业间交换命令 (Interindustry Command for Interchange)等内容进行标准化，其中 APDU交换应属于 OSI模型中的传输层，而行业间交换命令应属于应用层。

1 APDU交换

APDU交换是在链路层的 TPDU交换的基础上建立起来的，是行业间交换命令及应答的统一信息格式。用户可在下面的 API的基础上实现 IC支持的所有行业间交换命令。

extern char CardTypeAAPDUExchange(unsigned char CID, unsigned char NAD, unsigned char CLA, unsigned char INS, unsigned char P1, unsigned char P2, unsigned char Lc, unsigned char Data[], unsigned char Le, unsigned char Rec_Data[], unsigned short *Rec_Data_Length, unsigned char *SW1, unsigned char *SW2);

功用：由手持机向卡发送 APDU请求，并等待应答；

参数： unsigned char CID——由读写设备给非接触卡指定的 ID号 (0x00—0x0F)，用于区分处于活动状态 (Active State)的不同的 Mifare卡。不使用此功能可将参数置为 NoUsing

unsigned char NAD——用于标识读写设备与非接触卡之间的逻辑连接；不使用此功能可将参数置为 NoUsing

unsigned char CLA——命令 APDU的 CLA;

unsigned char INS——命令 APDU的 INS;

unsigned char P1——命令 APDU的 P1;

unsigned char P2——命令 APDU的 P2;

unsigned char Lc——命令 APDU的 Lc;

unsigned char Data[]——命令 APDU的 Data;

unsigned char Le——命令 APDU的 Le;

unsigned char Rec_Data[]——命令 APDU的应答数据；

unsigned short *Rec_Data_Length—命令 APDU的应答数据长度；

unsigned char *SW1——应答状态字；

unsigned char *SW2——应答状态字；

返回值： a. 正确执行，返回 MI_OK;

b. ISO14443—3A及其以下级别的错误 定义在 Mifare530. h中)；

c. ISO14443—4级别错误 定义在 TPDU_Layer(14443—4). h中)：

MI_TPDU_CRC_ERROR——TPDU层校验错；

MI_TPDU_EXCHANGE_ERROR——TPDU层帧交换错；

2 行业间交换命令

在这里利用上述 API实现两个基本的行业间交换命令：取随机数命令 (Get Challenge Command)和选择文件命令 (Select File Command)。用户可使用相同的方法实现其它的行业间交换命令。

(1) extern char GetChallenge(unsigned char CID, unsigned char NAD, unsigned char Length, unsigned char Challenge[]);

功用：由手持机向卡发送取随机数命令请求，并等待应答；

参数： unsigned char CID——由读写设备给非接触卡指定的 ID号 (0x00—0x0F)，用于区分处于活动状态 (Active State)的不同的 Mifare卡。不使用此功能可将参数置为 NoUsing

unsigned char NAD——用于标识读写设备与非接触卡之间的逻辑连接；不使用此功能可将参数置为 NoUsing

unsigned char Length——用于指定所取随机数长度；

unsigned char Challenge[]——用于存放返回的随机数。

返回值： a. 正确执行，返回 MI_OK;

b. ISO14443—3A及其以下级别的错误 定义在 Mifare530. h中)；

c. ISO14443-4级别错误 定义在 TPDU_Layer(14443-4).h中):

MI_TPDU_CRC_ERROR————TPDU层校验错;

MI_TPDU_EXCHANGE_ERROR——TPDU层帧交换错。

d. ISO7816-4级别 APDU交换错 定义在 APDU_Layer(7816-4).h中):

MI_APDU_EXCHANGE_ERROR——APDU交换错。

(2) extern char SelectFile(unsigned char CID, unsigned char NAD, unsigned char Select_Mode, unsigned char *FileName, unsigned char Rec_Data[], unsigned short *Rec_Length);

功用: 在逻辑通道上设置一个当前文件, 后续命令通过此逻辑通道提交给当前文件;

参数: unsigned char CID————由读写设备给非接触卡指定的 ID号 (0x00-0x0F), 用于区分处于活动状态 (Active State)的不同的 Mifare卡。不使用此功能可将参数置为 NoUsing

unsigned char NAD————用于标识读写设备与非接触卡之间的逻辑连接; 不使用此功能可将参数置为 NoUsing

unsigned char Select_Mode ——用于指定命令模式 (0x04为使用文件名形式);

unsigned char *FileName ————用于指定所选择的文件名;

unsigned char Rec_Data[]————命令返回数据;

unsigned short *Rec_Length——命令返回数据长度;

返回值: a. 正确执行, 返回 MI_OK;

b. ISO14443-3A及其以下级别的错误 定义在 Mifare530.h中);

c. ISO14443-4级别错误 定义在 TPDU_Layer(14443-4).h中):

MI_TPDU_CRC_ERROR————TPDU层校验错;

MI_TPDU_EXCHANGE_ERROR——TPDU层帧交换错。

d. ISO7816-4级别 APDU交换错 定义在 APDU_Layer(7816-4).h中):

MI_APDU_EXCHANGE_ERROR——APDU交换错。

三、参考资料

(1) ***<<智能卡技术--IC卡>>***----------清华大学出版社;

(2) ***<<IC卡的技术与应用>>***----------电子工业出版社

(3) ≪ MC2002 Hand-Held Smart Card Read/Write Device (RWD) Optional Device Library Manual: MIFARE® Accessing Library ≫