ICS 35.240.40
A11

JR

中 华 人 民 共 和 国 金 融 行 业 标 准

JR/T XXXXX—XXXX

中国金融移动支付 安全单元
第1部分：通用技术要求

China financial mobile payment--Secure Element--
Part 1: General technical requirements

（报批稿）

（本稿完成日期：2012年10月22日）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中国人民银行　发布

目　　次

前　言

《中国金融移动支付 安全单元》标准由以下 2 部分构成：
——第 1 部分：通用技术要求；
——第 2 部分：多应用管理规范；
本部分为该标准的第 1 部分。
本部分按照 GB/T 1.1-2009 给出的规则起草。
本部分由中国人民银行提出。
本部分由全国金融标准化技术委员会（SAC/TC180）归口。
本部分负责起草单位：。
本部分参加起草单位：。
本部分主要起草人：。

引　　言

随着移动支付新业务、新产品、新管理模式的不断涌现，出现了若干满足客户需求的移动支付产品。由于移动支付产业链长，应用复杂，涉及到不同机构、不同业务的多种产品形态，因此有必要对移动支付产品的技术要求进行规定。

移动支付安全单元是构成移动支付产品的主要组成部分。为确保各机构在开发应用移动支付产品时，具有统一的依据，本标准对移动支付安全单元的物理特性、电气特性、通信协议、工作模式等进行了规定。

中国金融移动支付 安全单元 第1部分：通用技术要求

1 范围

标准本部分对移动支付产品和安全单元提出了通用技术要求，主要包括物理特性、电气特性、逻辑接口、通讯协议和工作模式等。

标准本部分适用于从事移动支付业务的集成电路(IC)、智能卡产品的设计、制造、以及相关应用系统的研制、开发、集成和维护的相关单位。

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，仅所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。

GB/T 16649 识别卡 带触点的集成电路卡

JR/T XXXXX 中国金融移动支付 非接触式接口规范

ISO/IEC 28361 Near Field Communication Wired Interface (NFC-WI)

ETSI TS 102 613 Smart Cards: UICC - Contactless Front-end (CLF) Interface; Part 1: Physical and data link layer characteristics

ETSI TS 102 622 Smart Cards: UICC - Contactless Front-end (CLF) Interface; Host Controller Interface (HCI)

ETSI TS 102 221 Smart Cards; UICC-Terminal interface; Physical and logical characteristics

3 术语和定义

JR/T XXXX 《中国金融移动支付 应用基础 第1部分：术语》中界定的以及下列术语和定义适用于本文件。

3.1

主机控制接口(HCI) host controller interface(HCI)

主机控制接口(HCI)定义了主机之间用来传输命令、响应、事件的门，消息传播机制和主机之间的消息路由。

4 符号和缩略语

4.1 符号

t_F	Fall time	下降时间
t_R	Rise time	上升时间
Vcc	Supply Voltage	VCC 上的电源电压
V_{OH}	High Level Output Voltage	输出高电压（高）

V_{OL}	Low Level Output Voltage	输出低电压（低）
V_{IH}	High Level Input Voltage	输入高电压（高）
V_{IL}	Low Level Input Voltage	输入低电压（低）
I_H	Input High Current	输入高电流
I_L	Input Low Current	输入低电流

4.2 缩略语

(U)SIM	(Universal) Subscriber Identity Module	通用用户身份识别模块
NFC-WI	Near Field Communication Wired Interface	近场通信有线接口

5 移动支付安全单元

5.1 基于 SWP 接口(U)SIM 卡

5.1.1 物理特性

(U)SIM 卡的物理特性应符合 GB/T 16649.1 的要求。

5.1.2 接触通道的电气特性和传输协议

(U)SIM 卡的接触通道的接口电气特性和传输协议应符合 GB/T 16649.2 和 GB/T 16649.3 的要求。

5.1.3 非接触通道的电气特性和传输协议

非接触通道的电气特性和传输协议参见 JR/T XXXXX《中国金融移动支付 非接触式接口规范》。

5.1.4 安全单元逻辑结构

(U)SIM 卡安全单元包括接触通道和非接触通道，接触通道和非接触通道应具有并发处理能力，并互不影响。

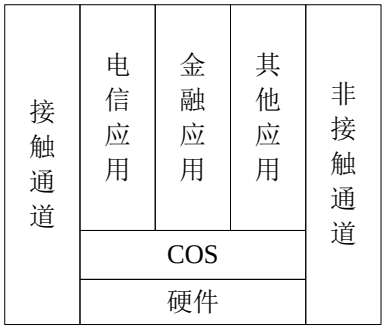

图 1 (U)SIM 卡逻辑结构图

5.1.5 基于 SWP 接口的(U)SIM 卡扩展接口定义

5.1.5.1 硬件结构

基于SWP接口(U)SIM移动支付方案的核心部分包括天线、非接触射频前端(CLF)、基于SWP接口(U)SIM，可以在移动终端上实现非接触IC卡卡片功能。

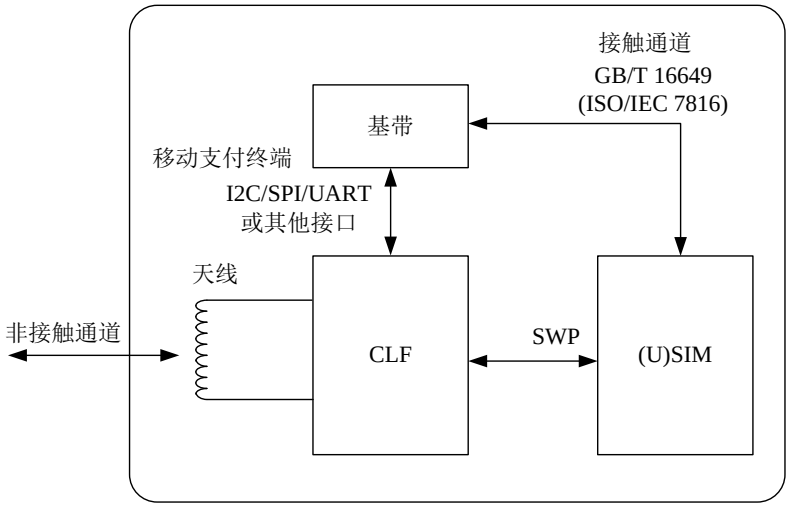

图 2 基于 SWP 接口(U)SIM 移动支付方案结构图

5.1.5.2 电源管理

当移动终端开机时，或关机但电池仍能通过电源管理系统正常提供电源能量时，(U)SIM可使用移动终端的电池作为电源能量；当移动终端的电池被取下时，或电池无法通过电源管理系统正常提供电源能量时，(U)SIM应选择使用CLF芯片从受理终端的工作场中感应得到的电源能量。

在(U)SIM可获得正常工作所需的电源能量的情况下，应能正常执行金融应用。

5.1.5.3 (U)SIM 卡触点定义

(U)SIM卡的触点分布如图3所示，其中C6用于SWP接口通信：

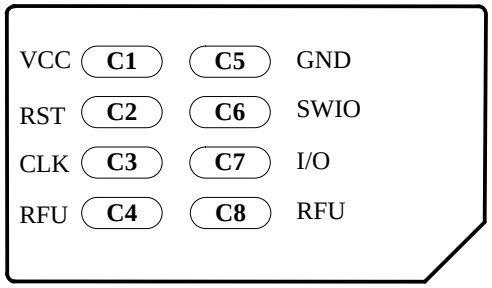

图 3 (U)SIM 卡触点

(U)SIM卡触点定义如表1所示：

表 1 (U)SIM 卡的触点定义

管脚号	名称	类型	描述
C1	VCC	P	电源电压
C2	RST	I/O	复位
C3	CLK	I/O	时钟
C4	RFU	-	未使用
C5	GND	I	地
C6	SWIO	I/O	SWP 接口

C7	I/O	I/O	数据线
C8	RFU	-	未使用

5.1.5.4 单线协议

5.1.5.4.1 单线协议基本原理

CLF和(U)SIM卡之间应采用单线协议（Single Wire Protocol，简称SWP）连接，单线协议接口的电气特性和链路层传输协议应分别符合ETSI TS 102 613 V8.0及以上版本的要求，其传输层协议应满足ETSI TS102 622 V8.0及以上版本的要求。

CLF与基带之间的接口可为I2C、SPI或UART，本标准不作限定。

SWP接口是一种(U)SIM卡与非接前端之间面向比特流、点对点的通讯协议，如图4所示。CLF是主设备、(U)SIM是从设备。

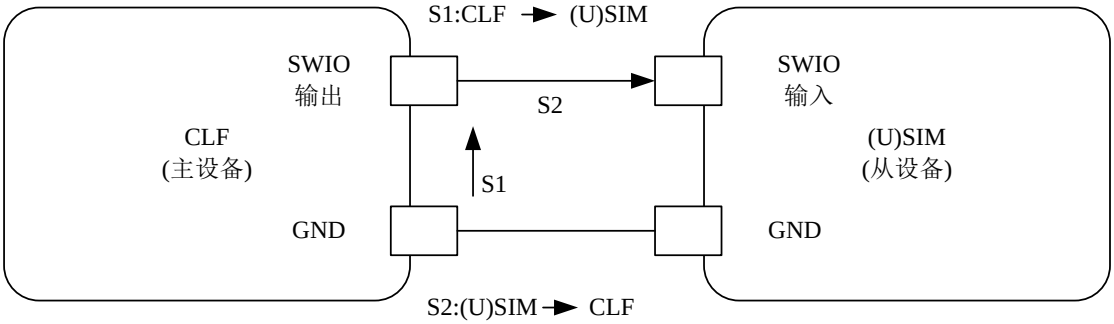

图 4 SWP 数据传输

SWP协议基于全双工数字传输模式：

——S1信号通过一个数字模块发送的电压信号传输；

——S2信号通过一个数字模块发送的电流信号传输。

当主设备以高状态发送S1信号，从设备借助上拉电流（高状态）或不借助上拉电流（低状态）来传输S2信号。因S1以脉冲宽度编码，所以可以在它上面传送一个传输时钟，即数据以全双工模式传输。只有在S1处于高状态时S2才有效。

5.1.5.4.2 单线协议电气特性

非接前端的电压值和(U)SIM S1信号的电压值在图5中表征。

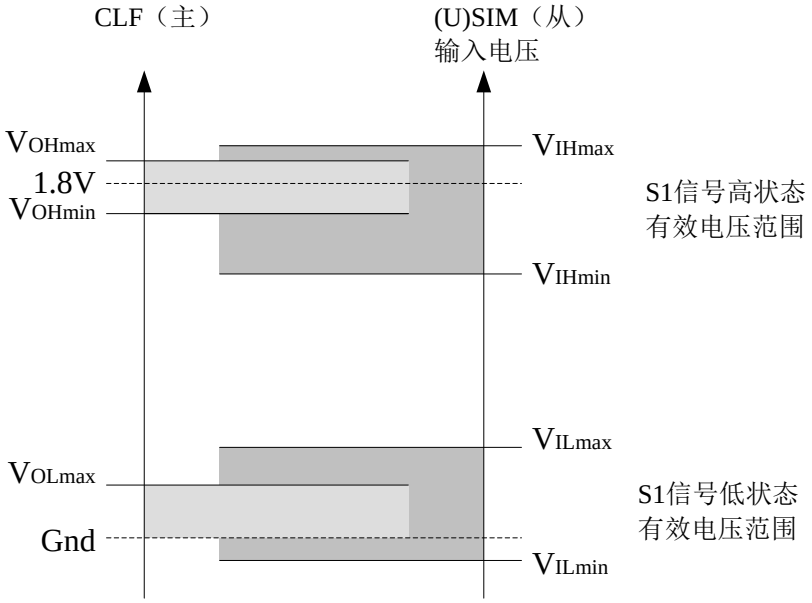

图 5 S1 信号的电压定义

Vih和Vil表示由从设备接收到的电压。Voh和Vol表示由主设备发送出的电压。所有的电压值都相对接地的电压值。

SWP接口适用另一个S2信号，它是主设备到从设备的一个电流信号，同时允许从设备在之上返回数据给主设备。S2信号的值只有在S1信号为高时有效。S2信号的电流值定义在5.1.5.5.6中，由图6给出。

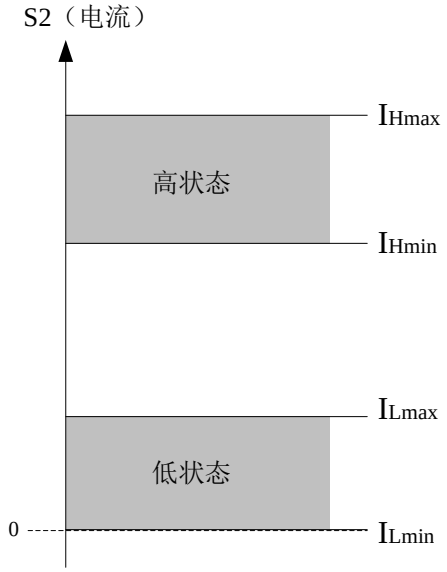

图 6 SWIO 上 S2 信号的电流值定义

5.1.5.4.3 提供的电压级别

一个支持SWP接口的(U)SIM卡应当支持ETSI TS 102 221中定义的B类电压和C类电压。

5.1.5.4.4 S1 信号

S1是一个电压域的值，用来从非接前端向(U)SIM在SWIO（触点C6）上传送数据。

S1和S2信号共享一个电气触点。S1的电气特征在表2和表3中给出。

表 2 SWIO 上 S1 信号在正常 B 类条件下的电气特征

标记	参数	条件	最小值	最大值	单位
V_{OH}	输出高电压（高）	$I_{L\ min} \le I \le I_{H\ max}$	1.40	1.98（见备注）	V
V_{OL}	输出低电压（低）	-20 μA ≤ I ≤ 20 μA	0（见备注）	0.3	V
V_{IH}	输入高电压（高）		1.13	2.28（见备注）	V
V_{IL}	输入低电压（低）		-0.3	0.48	V
备注：在动态工作的情况下，允许SWIO上的超限电压值为-0.3V和V_{CC}+ 0.3V之间 备注：$I_{L\ min}$,$I_{H\ max}$的值在5.1.5.5.6中给出					

表 3 SWIO 上 S1 信号在正常 C 类条件下的电气特征

标记	参数	条件	最小值	最大值	单位
V_{OH}	输出高电压（高）	$I_{L\ min} \le I \le I_{H\ max}$	0.85 x V_{CC}	V_{CC}（见备注）	V
V_{OL}	输出低电压（低）	-20 μA ≤ I ≤ 20 μA	0（见备注）	0.15 x V_{CC}	V
V_{IH}	输入高电压（高）		0.7 x V_{CC}	V_{CC}+0.3	V
V_{IL}	输入低电压（低）		-0.3	0.25 x V_{CC}	V
备注：在动态工作的情况下，允许SWIO上的超限电压值为-0.3V到V_{CC}+ 0.3V之间 备注：$I_{L\ min}$, $I_{H\ max}$的值在5.1.5.5.6中给出					

5.1.5.4.5 S2 信号

S2信号是一个电流域的值，用来从(U)SIM发送数据到主设备。

S2和S1信号共享一个电气触点C6。S2信号的电气特征在本节被描述。

5.1.5.4.6 S2 的工作条件

SWIO上S2信号在正常条件下的电气特性见表4。

当SWIO上的电流处于Ihmin和Ihmax之间，S2信号被认为处于高状态；

当SWIO上的电流处于Ilmin和Ilmax之间，S2信号被认为处于低状态。

表 4 SWIO 上 S2 信号在正常条件下的电气特征

标记	参数	条件	最小值	最大值	单位
I_H	高电流	$V_{IHmin} \le S1 \le V_{IHmax}$	600	1000	μA
I_L	低电流	$V_{IHmin} \le S1 \le V_{IHmax}$	0	20	μA

5.1.5.4.7 S1 信号的位编码和采样时序（自同步编码）

S1信号的位编码在图7中描述。

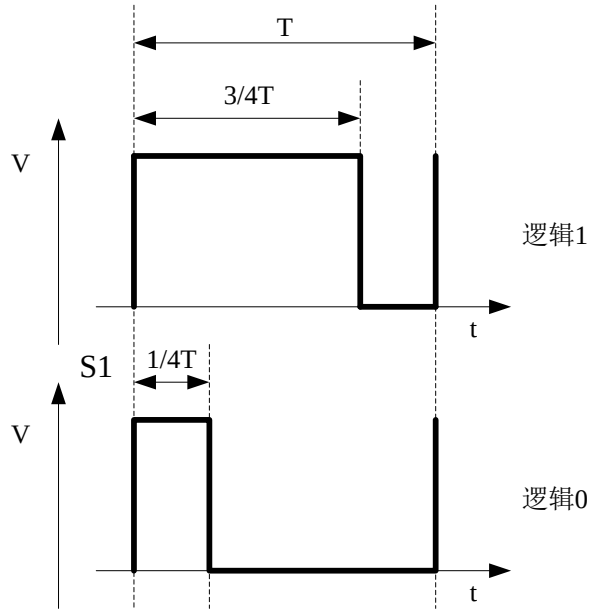

图 7 S1 信号的位编码

逻辑1的高状态持续时间是0.75T，逻辑0的高状态持续时间是0.25T。

所有的位都顺序传输。一个位被定义为有两个上升沿。

上升沿构成了一个位的开始和结束。每一个传输位的位持续时间都可以是不同的。

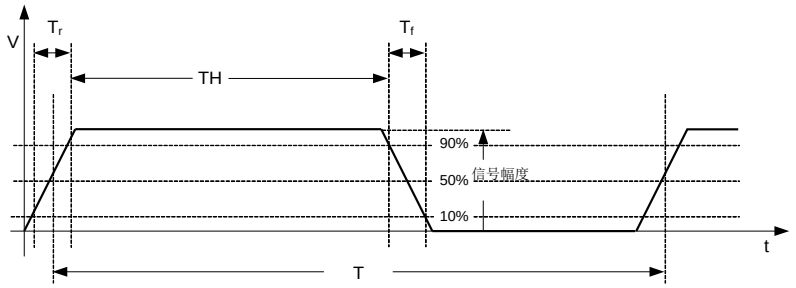

图 8 S1 信号的波形

(U)SIM在C6触点上的输入电容不应该超过10pF。

表 5 S1 信号的波形时序

标记	参数	条件	最小值	一般值	最大值	单位
t_F	下降时间	$C_{LOAD} \leq 10$ pF T < 5 000 ns	5 ns	-	0.05 x T	
		$C_{LOAD} \leq 10$ pF T > 5 000 ns	5 ns	-	250 ns	
t_R	上升时间	$C_{LOAD} \leq 10$ pF T < 5 000 ns	5 ns	-	0.05 x T（见备注1）	
		$C_{LOAD} \leq 10$ pF T > 5 000 ns	5 ns	-	250ns（见备注1，2）	
T_{H1}	S1信号逻辑1编码的高状		0.70 x T	0.75 x T	0.80 x T	

标记	参数	条件	最小值	一般值	最大值	单位
	态持续时间					
T_{H0}	S1信号逻辑0编码的高状态持续时间		0.20 x T	0.25 x T	0.30 x T	
T	默认位持续时间		1	-	5	μs
	扩展位持续时间		0.590	-	10	μs
备注1：对每个位开始和结束边沿有效 备注2：这些时间值应该也适用于SWIO的激活，传输及去激活状态						

5.1.5.4.8 S2 信号的切换管理

S2信号只有当S1信号处于高状态时有效。(U)SIM卡应当在S1处于低状态时才切换S2信号。或者当重新恢复SWP时，S2也允许切换，同时由于SWIO处于SUSPENDED 状态，S1处于H状态。

图9表明了S2信号相对S1信号的切换时序。

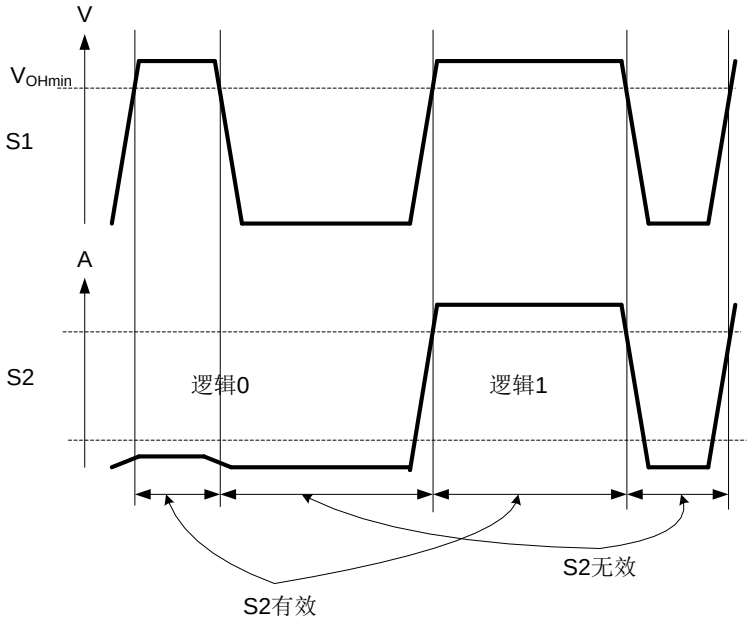

图 9 S2 信号的时序

5.1.5.4.9 SWP 接口状态管理

SWP有三种状态：

a) 激活状态：

在这种状态下主设备和从设备之间发送位数据。

b) 挂起状态：

在这种状态下S1处于高状态S2处于低状态。这种状态是SWP接口被激活后的初始状态。SWP维持这种状态直到唤醒或者去激活过程发生。

c) 非激活状态：

在这种状态下S1和S2都处于低状态。

SWP维持此状态直到激活过程发生。

在这些状态下相互切换的定义如下：

a） 唤醒：

从挂起状态到激活状态的切换过程。主设备和从设备都能发起唤醒过程使SWP进入激活状态。

主设备通过发送P2个连续的闲置位来发起唤醒过程。

SWP在这些位发送后进入激活状态。

从设备发起的唤醒过程是在电流上拉高（S2信号处于高状态）。

主设备应当发送在低于P3max的时间内发送一个序列来作为响应。在这个序列结束时，SWP进入激活状态。

从这个序列之后的延时到从设备发送的SOF帧之间不应该超过4个位。

如果主设备发起了唤醒，从设备应当在P2个空闲位后开始发送帧数据。

b） 挂起：

如果在SWP上持续P1时间内没有数据交互，主设备可以将SWP切换到挂起状态，

通过维持S1信号处于高状态。

c） 去激活：

如果SWP处于挂起状态，主设备可以将SWP切换到非激活状态，

通过维持SWIO处于低状态超过P4时间。

d） 激活：

如果SWP处于非激活状态，被唤醒后执行唤醒流程。

从设备可以通过使用在ETSI TS 102 223中描述激活接口命令来激活SWP接口。

图10描述了SWP接口上活动的一个例子。

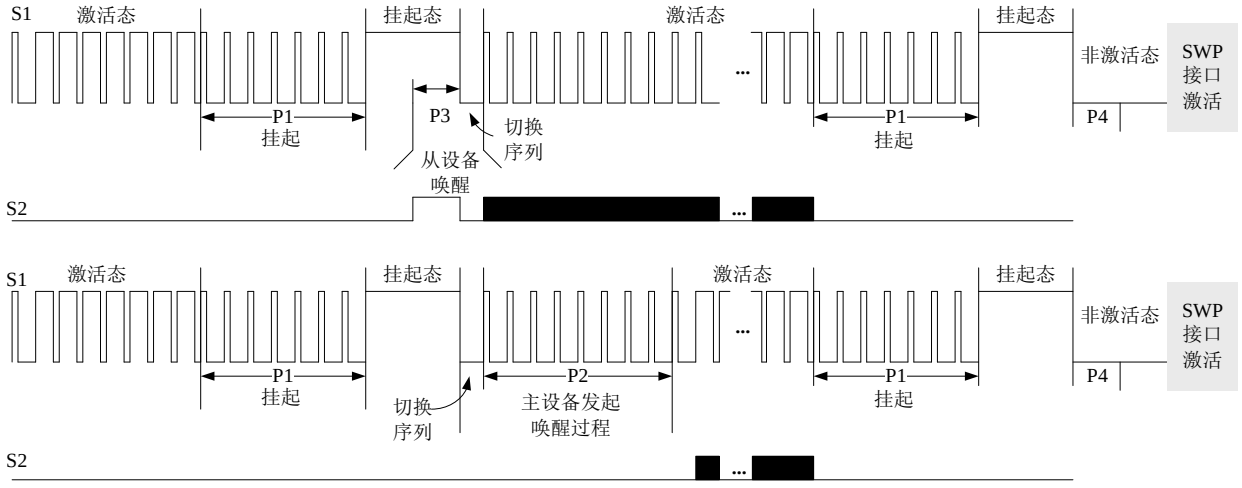

图10 SWP状态及其切换

表6给出了SWP的时序管理。

表 6 SWP 时序管理

标记	参数	最小值	最大值	单位
P1	挂起序列	7	-	比特
P2	主设备唤醒序列	8	8	比特
P3	从设备唤醒时间	-	5	μs
P4	去激活时间	100	-	μs

标记	参数	最小值	最大值	单位
Px	SWP非活动超时	15		ms

5.2 全终端

5.2.1 物理特性

本标准不作限定。

5.2.2 接触通道的电气特性和传输协议

移动终端内置安全单元下，CLF和安全单元（SE)接口是内部接口，可采用SWP、NFC-WI及其它内部接口协议。单线协议（SWP）接口的电气特性和链路层传输协议应分别符合ETSI TS 102 613的要求，其传输层协议应满足ETSI TS 102 622的要求。NFC-WI的电气特性和链路层传输协议应符合ISO/IEC 28361的要求。

CLF与基带的接口本规范不作限定。

5.2.3 非接触通道的电气特性和传输协议

非接触通道的电气特性和传输协议参见《中国金融移动支付 非接触式接口规范》。

5.2.4 安全单元逻辑结构

全终端方案所用的安全单元包括接触通道和非接触通道，接触通道和非接触通道应具有并发处理能力，并互不影响。

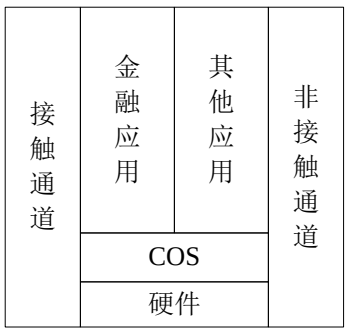

图 11 全终端安全单元逻辑结构图

5.2.5 全终端方案接口定义

5.2.5.1 硬件结构

全终端方式的移动支付方案的核心部件至少包含CLF、内置安全芯片、天线等模块，如图12所示：

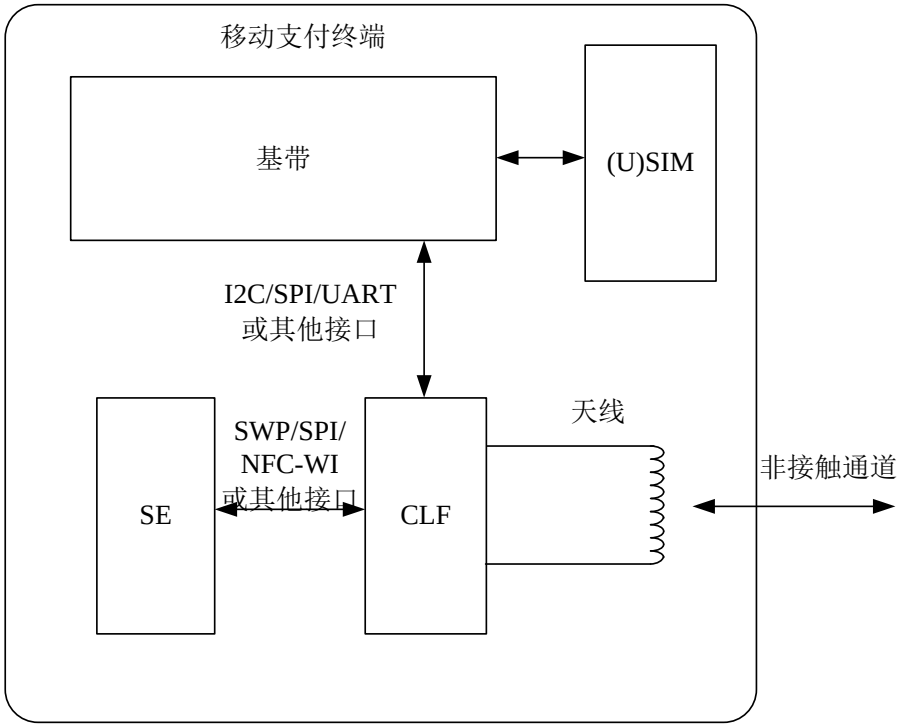

图 12 全终端移动支付方案结构图

5.2.5.2 电源管理

当移动终端开机时，或关机但电池仍能通过电源管理系统正常提供电源能量时，安全芯片安全单元（SE)可使用移动终端的电池作为电源能量；当移动终端的电池被取下时，或电池无法通过电源管理系统正常提供电源能量时，安全芯片安全单元（SE)应选择使用CLF芯片从受理终端的工作场中感应得到的电源能量。

在安全芯片安全单元（SE)获得正常工作所需的电源能量的情况下，应能正常执行金融应用。

5.2.5.3 全终端安全单元尺寸

本规范不作限定。

5.2.5.4 全终端安全单元触点定义

本规范不作限定。

5.3 基于 SWP 接口的智能 SD 卡

5.3.1 物理特性

基于SWP接口的智能SD卡，除SWP接口外，物理特性应符合《SD Card Specification》 V2.0或以上版本的要求。

5.3.2 接触通道接口的电气特性和传输协议

基于SWP接口的智能SD卡，除SWP接口外，接触通道接口的电气特性应符合《SD Card Specification》V2.0或以上版本的要求。

5.3.3 非接触通道的电气特性和传输协议

非接触通道的电气特性和传输协议参见JR/T XXXXX《中国金融移动支付 非接触式接口规范》。

5.3.4 安全单元逻辑结构

基于 SWP 接口的智能 SD 卡安全单元包括接触通道和非接触通道，接触通道和非接触通道应具有并发处理能力，并互不影响。

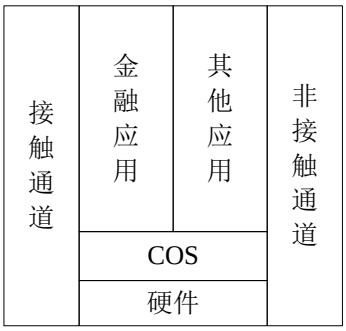

图 13 基于 SWP 接口的智能 SD 卡逻辑结构图

5.3.5 基于 SWP 接口的智能 SD 卡扩展接口定义

5.3.5.1 硬件结构

基于SWP接口的智能SD卡移动支付方案的核心部分包括射频天线、非接触射频前端（CLF）、基于SWP接口的智能SD卡，可以在移动终端上实现非接触IC卡卡片功能，硬件结构如图14所示：

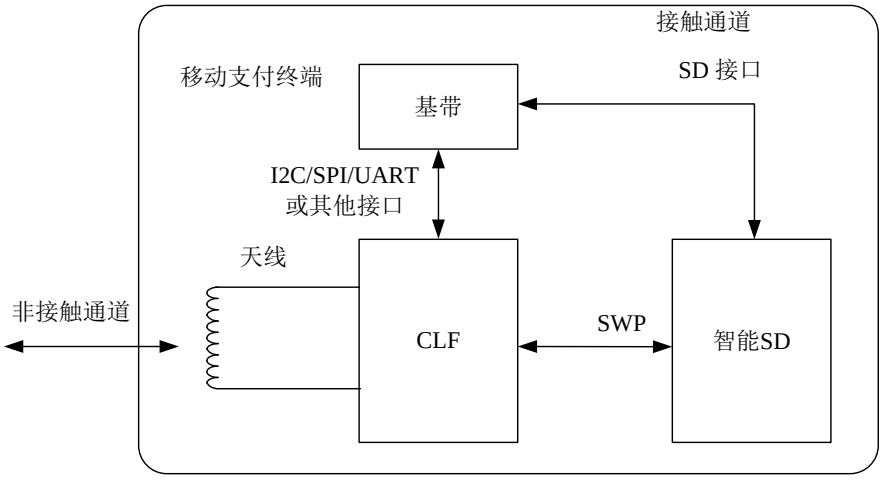

图 14 基于 SWP 接口的智能 SD 卡方案结构图

基于SWP接口的智能SD卡与CLF芯片之间应采用SWP接口连接，智能SD卡和CLF芯片的SWP接口的电气特性和链路层传输协议应分别符合ETSI TS 102 613 V8.0及以上版本的要求，其传输层协议应满足 ETSI TS 102 622 V8.0及以上版本的要求。

CLF与基带之间的接口可为I2C、SPI或UART，本标准不作限定。

5.3.5.2 电源管理

当移动终端开机时，或关机但电池仍能通过电源管理系统正常提供电源能量时，基于SWP接口的智能SD卡中的安全单元（SE)可使用移动终端的电池作为电源能量；当移动终端的电池被取下时，或电池无法通过电源管理系统正常提供电源能量时，智能SD卡中的安全单元（SE)应选择使用CLF芯片从受理终端的工作场中感应得到的电源能量。

在基于SWP接口的智能SD卡中的安全单元（SE)获得正常工作所需的电源能量的情况下，应能正常执行金融应用。

5.3.5.3 基于 SWP 接口的智能 SD 卡尺寸

基于SWP接口的智能SD卡标准触点的尺寸及卡片整体的机械特性描述和尺寸规格参见《SD Card Specification》 V2.0，机械特性描述如图15所示，对应的尺寸规格如表7所示：

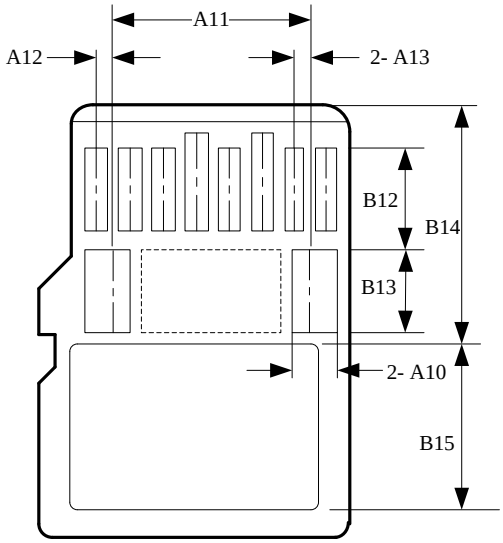

图 15 智能 SD 卡机械特性描述

表 7 基于 SWP 接口的智能 SD 卡片尺寸规格

	通用尺寸（mm）		
标号	最小值	平均值	最大值
A10	1.35	1.40	1.45
A11	6.50	6.60	6.70
A12	0.50	0.55	0.60
A13	0.40	0.45	0.50
B12	3.60	3.70	3.80
B13	2.80	2.90	3.00
B14	8.20	-	-
B15	-	-	6.20

5.3.5.4 基于 SWP 接口的智能 SD 卡触点定义

基于SWP接口的智能SD卡触点分布见图16，其中《SD Card Specification》中的两个RF PIN在本方案中被扩展为SWP(Pin 9)和VCCSWP(Pin 10)。

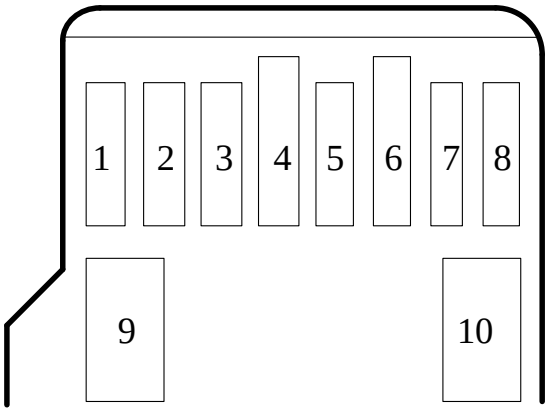

图 16 基于 SWP 接口的智能 SD 卡触点

基于SWP接口的智能SD卡触点定义如表8所示：

表 8 基于 SWP 接口的智能 SD 卡触点定义

Pin#	名称	类型	描述
1	DAT2	I/O	数据线[Bit 2]
2	CD/DAT3	I/O	卡片侦测/数据线[Bit 3]
3	CMD	P	指令/响应
4	VCC	P	供电电压
5	CLK	I	时钟
6	VSS	G	接地
7	DAT0	I/O	数据线[Bit 0]
8	DAT1	I/O	数据线[Bit 1]
9	SWP	I/O	SWP 数据线
10	VCCSWP	P	来自于 CLF 的供电电压
备注：类型符号定义：P 电源；G 地；I 输入；O 输出；I/O 输入/输出			

5.3.6 SD 安全控制器芯片

基于SWP接口的智能SD卡内部结构见图17。基于SWP接口的智能SD卡中的SD控制器芯片应具有接触式接口与安全芯片安全单元（SE)连接，本规范对此接口不作限定。基于SWP接口的智能SD卡中的SD控制器芯片的SD接口应符合《SD Card Specification》V2.0或以上版本的要求。基于SWP接口的智能SD卡应具有SWP接口与SD卡中的安全芯片安全单元（SE)连接。基于SWP接口的智能SD卡中的SD控制器芯片与flash存储器的接口本规范不作限定。

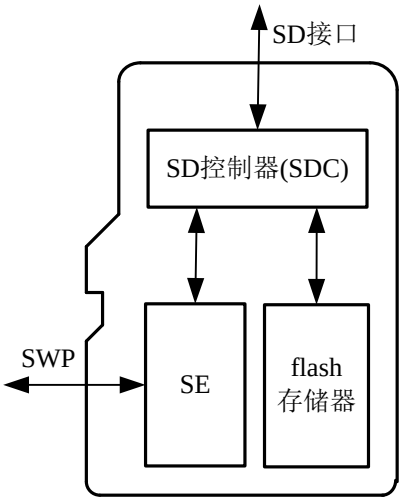

图 17 基于 SWP 接口的智能 SD 卡内部结构

5.3.7 基于 SWP 接口的智能 SD 卡逻辑接口

5.3.7.1 概述

本节主要规定了智能SD卡与移动终端之间的逻辑接口和交互流程。

对嵌入在智能SD卡内的智能卡芯片操作可以通过作为接触通道和非接触通道两个接口进行，本节仅描述通过接触通道来操作智能卡芯片的方式和机制。

应用接口支持两种方式，一是单文件方式，一是多文件方式；这些文件定义为智能SD卡接口文件(SCIF)。

单文件方式：在智能SD卡存储区的根目录上存在一个文件，这个文件预先和嵌入在智能SD卡内的安全芯片关联。

多文件方式：在智能SD卡存储区的根目录上存在一个文件夹，该文件夹中预置多个文件，这些文件预先和嵌入在智能SD卡内的安全芯片关联。

5.3.7.2 接口文件定义

单文件方式下的文件名定义为“MPAYSSD0.SYS”，并具有如下属性和特征：

存在于智能 SD 卡文件系统的根目录下

——建议智能 SD 卡文件系统支持 FAT16 或 FAT32 文件系统；

——隐藏文件；

——以二进制方式操作；

——长度为 512 字节的整数倍；

——考虑到某些手机操作系统不能对设为“系统属性”的文件进行读写操作，接口文件不能设为“系统属性”。

多文件方式下的文件夹（SDIF）定义为“MPAYSSD”，并具有如下属性和特征：

——存在于智能 SD 卡文件系统的根目录下；

——建议智能 SD 卡文件系统支持 FAT16 或 FAT32 文件系统；

——以二进制方式操作；

——每个文件的长度为 512 字节的整数倍；

——不能设为“系统属性”；

——命名规则从 MPAYXX.SYS，其中 xx 的编码从 00h～FFh。文件夹下文件数目最大不超过 256 个。

接口文件不应对智能 SD 卡的正常使用寿命造成影响，且接口文件应具有下述自我保护功能：

——自我保护功能是指用户对于智能 SD 卡进行任何的正常操作，都不能破坏智能 SD 卡应用接口，或对 SD 卡的正常功能造成损害从而影响用户的正常使用，如：文件系统混乱等；

——自我保护功能不应限制用户对 SD 卡的正常操作，如：格式化、读写文件、删除文件等。

终端应该首先在根目录下搜索是否存在 SCIF 文件，如果不成功则在根目录下搜索 SDIF 文件夹。如果不成功，则终止程序。表明该 SD 卡不支持本规范定义的接口，如果存在则继续通过该接口操作。

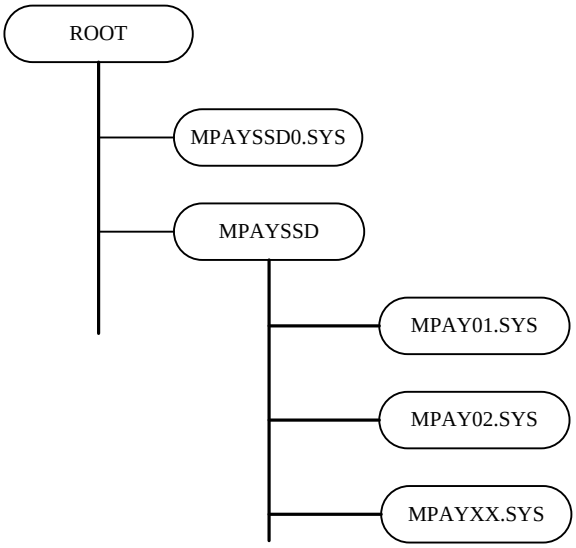

图 18 文件接口示意图

5.3.7.3 智能 SD 卡的状态转换

嵌入在智能SD卡内的安全芯片和SD卡控制器(SDC)相连，智能SD卡应该按照如下状态工作：

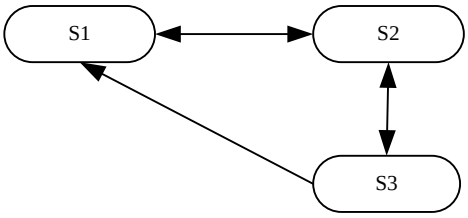

图 19 智能 SD 卡的状态转化图

各个状态的描述如表 9 所示。智能 SD 卡初始阶段处于 S1 状态，之后按照状态图进行转换。

表 9 智能 SD 卡的状态转换

状态	描述	状态转换	
		指令	后续状态
S1	下电状态，这是智能 SD 卡的初始或缺省状态	SCIF_CONNECT	S2
S2	上电状态，SDC 建立并维持和安全单元（SE)的通讯状态	SCIF_ATR SCIF_PPS SCIF_DISCONNECT SCIF_INFO	S3 S2 S1 S2

S3	命令交互状态	SCIF_ATR	S3
		SCIF_APDU	S3
		SCIF_INFO	S3
		SCIF_DISCONNECT	S1

5.3.7.4 对接口文件的操作与智能 SD 卡操作的对应关系

对 SCIF 文件的操作通常按如下顺序进行，只有在文件的写操作才对应到对智能 SD 卡的操作，SD 控制器必须将写入文件的内容按照 5.3.7.9 节的协议解析出命令，并进行相应的处理；响应信息和响应代码一起作为 SCIF 文件的内容供外部应用读取。

响应信息和响应代码的编码方式见后续章节，整个响应信息位于 SCIF 文件的起始位置，即偏移量为 0 的位置。

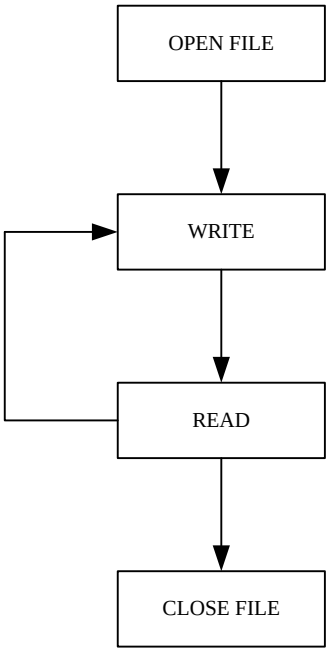

图 20 智能 SD 卡文件操作流程

打开 SCIF 文件和关闭 SCIF 文件只是在宿主操作系统中分配适当的资源并在应用软件和智能 SD 卡间建立关联关系，并没有具体的动作和安全芯片关联。

智能 SD 卡根据一定的格式解析准备写入的数据，并按如下步骤进行处理：

a) 检测终端应用程序（TA）写下来的命令数据包的会话流水号是否出现异常，如果出现异常，返回异常状态给 TA。

b) 对写下来的数据包进行数据校验，校验码不对就返回非法命令错误码：SCIF_IO_ILLEAGAL_CMD；

c) 识别并解析应用写入的数据包中的命令码，如果是请求安全芯片的复位信息，就对安全芯片进行复位，记录结果并返回，流程终止。

d) 如果是 APDU 命令，则转发 APDU 命令到智能 SD 卡内的安全芯片，记录本次内部通讯状态，如果通讯状态正常则接收智能卡返回的响应数据，将内部通讯状态码、安全芯片返回的状态码及安全芯片返回的数据按一定格式写入到 SCIF 文件中，准备被外部应用读取；并继续以下步骤，否则在文件内容中设置相应的错误代码并结束处理。

e) 如果是进行 PPS 交换，则按照定义的 PPS 命令和安全芯片进行 PPS 协商，并接收安全芯片返回的 PPS 协商结果。

5.3.7.5 发送序列计数器 SSC

发送序列计数器（Send Sequence Counter）是用来监控TA和SDC之间会话报文发送与接收顺序的计数器，其初始值由SDC随机生成并维护。其结构由两个字节构成，定义如表10所示：

表 10 SSC 的结构

MSB LSB

8	7	6	5	4	3	2	1		8	7	6	5	4	3	2	1	含义
0	0	0	0														会话标识
				x	x	x	x		x	x	x	x	x	x	x	x	会话流水号

会话流水号是 SDC 根据当前会话所分配的 SSC 的具体取值，其取值范围在（1~4095）。在 TA 发送 SCIF_CONNECT 指令（此时 SSC 中会话流水号为 0000）后，SDC 为本次会话生成一个初始的 SSC 并在响应报文中返回给 TA，其中初始会话流水号为取值范围内的一个随机值。TA 在每次收到响应报文中的 SSC 之后，必须递增其中的会话流水号取值，产生新的 SSC 之后作为下一个请求报文中的 SSC。如果会话流水号已达到最大值 4095，则递增后从 1 开始。

SDC 会检测 TA 请求报文中 SSC 的会话流水号是否出现异常，如果出现异常，则返回错误状态码 SCIF_SSC_ERROR。其中，TA 请求报文中 SSC 的会话流水号异常是如下定义的：

a) 发送了 SCIF_CONNECT 指令之后，TA 发送的第一个请求报文中的会话流水号必须是在 SDC 返回的初始会话流水号上递增 1，否则就视为异常；

b) SDC 收到 TA 的请求报文后，检查 SSC 的正确性。如果当前的请求报文中 SSC 的会话流水号和前一个请求报文中的会话流水号不是递增 1 的关系，且前一个会话流水号不是 4095 的话，则视为 SSC 异常；

c) TA 发送的请求报文（SCIF_CONNECT 指令除外）中 SSC 的会话流水号超出了 1~4095 的取值范围。

TA 也必需检测 SDC 返回的响应报文中 SSC 的会话流水号和自己请求报文中的会话流水号是否一致，如果不一致则认为是响应报文异常。TA 应采取一定的纠错措施，比如重新发送上一个请求报文，或者重新开始一次应用的会话过程。

5.3.7.6 写接口文件的格式

TA准备写入到智能SD卡的应用接口文件的数据按如表11格式组织：

表 11 应用接口文件写入内容格式

序号	偏移	字节长度	含义	存在方式
1	0	2	发送序列计数器 SSC	必须
2	2	2	命令码	必须
3	4	2	命令长度	必须
4	6	可变	APDU	条件存在
5		1	字节校验和（LRC）	必须

a) 命令码

命令码定义了对智能 SD 卡的操作类型，如表 12 所示：

表 12 写接口文件中的命令码

代码	值	含义
SCIF_INFO	00h 01h	取智能 SD 卡版本信息

代码	值	含义
SCIF_DISCONNECT	01h 01h	对安全芯片的下电通知
SCIF_CONNECT	01h 02h	对安全芯片的上电通知
SCIF_ATR	01h 03h	通知 SD 控制器读取上一次复位中缓存的安全芯片的 ATR 信息
SCIF_APDU	01h 04h	通知 SD 控制器转发 APDU 命令
SCIF_PPS	01h 05h	PPS 请求

b) 字节校验和

对从序号为 1～4 的数据逐字节异或，结果作为整个数据的校验数据。

c) 响应时间要求

符合《SD Specifications Part 1 Physical Layer Specification》中 4.6 节对写操作的最大等待时间的要求。

5.3.7.7 读接口文件的格式

只有发送了写命令以后，应用程序才可以去读该文件，从文件的内容中得知上次命令的处理结果或响应数据。读取的文件内容按表 13 解释。

表 13 智能 SD 卡读取内容格式

序号	偏移	字节长度	含义	存在方式
1	0	2	SSC	必须
2	2	2	通讯状态码	必须
3	4	2	响应数据长度	必须
4	6	xx	响应数据	条件存在
5	xx	1	字节校验和（LRC）	必须

a) 通讯状态码

通讯状态码定义了 SD 控制器和智能 SD 卡交互的通讯情况，应用程序必须首先识别该状态码是否正确，然后才能识别后续数据，通讯状态码按表 14 定义。

表 14 智能 SD 卡的通讯状态码

代码	值	含义	处理方式
SCIF_IO_OK	00 00h	通讯正常	正常的处理流程
SCIF_IO_ILLEAGAL_CMD	00 01h	非法命令	按照 5.3.7.6（1）节描述检查命令码是否有效，如无效，则改为正确的命名码并重新发送请求报文
SCIF_IO_TIMEOUT	00 02h	通讯超时	发送 SCIF_DISCONNECT 指令使智能 SD 卡回到初始状态 S1
SCIF_IO_ERROR	00 03h	通讯失败	发送 SCIF_DISCONNECT 指令使智能 SD 卡回到初始状态 S1
SCIF_IO_BUSY	00 04h	SDC 忙	重新发送读操作指令，以获取正确的响应数据
SCIF_ILLEAGAL_STATUS	00 05h	非法状态	检查当前状态，参见 5.3.7.3 节描述，发送相应的指令使智能 SD 卡进入到正确的状态
SCIF_SSC_ERROR	00 06h	会话流水号异常	按照 5.3.7.5 节描述修改为正确的会话流水号并重新发送请求报文

b) 字节校验和

对从序号为 1～4 的数据逐字节异或，结果作为整个数据的校验数据。

c) 响应时间要求

符合《SD Specifications Part 1 Physical Layer Specification》中 4.6 节对读操作的最大等待时间的要求。

5.3.7.8 应用流程

TA 通过 SDC 访问安全芯片安全单元（SE)，必须按如下流程来访问：

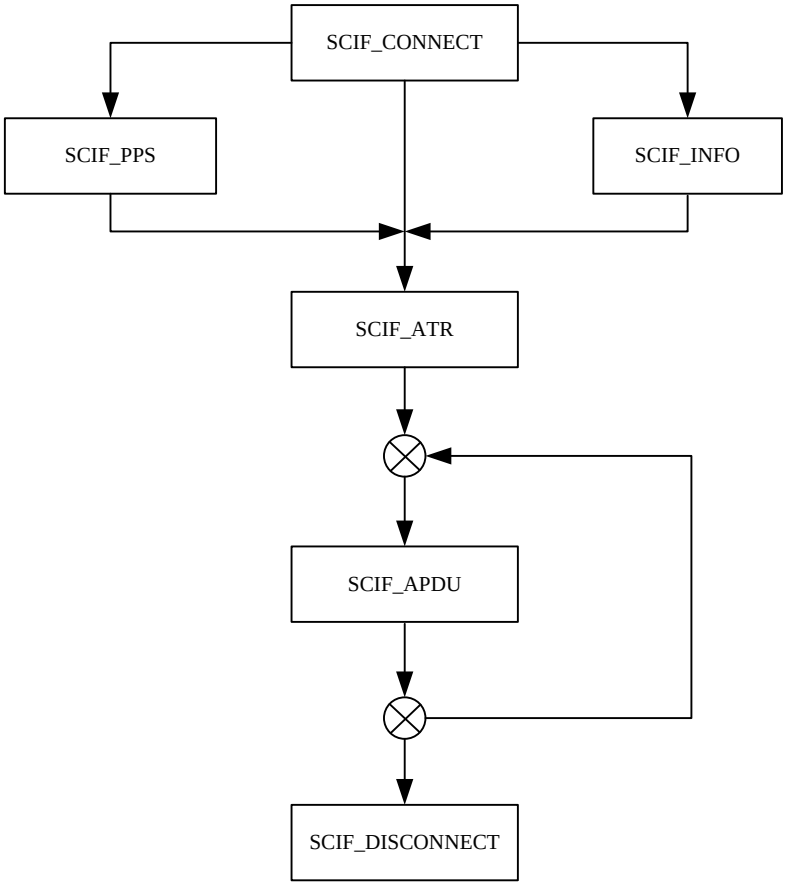

图 21 应用流程示例

当 TA 发送 SCIF_CONNECT 指令后，SDC 为该终端应用程序分配一个会话标识，表示当前的通信连接。当 TA 发送 SCIF_DISCONNEC 指令结束当前与卡片的通信连接，SDC 销毁此次会话标识。TA 必须遵循图 21 的流程来访问卡片，其中 SCIF_APDU、SCIF_PPS 和 SCIF_INFO 是可选步骤，其他是必须步骤。如果 TA 不遵循此步骤执行，SDC 会返回卡片状态字标识“非法状态”。

其中 SCIF_PPS 可以用来改变 SDC 和安全芯片之间的通信协议和通信速率，智能 SD 卡可选支持此功能。

指令序列交互流程：

a) 终端应用程序（TA）向 SDC 发送命令。
b) 终端应用程序（TA）向 SDC 读取响应，读取响应的时机可以采用不同的方法来决定，比如采用循环查询的机制，直到读取响应码或超时结束；或者 TA 根据智能 SD 卡处理命令的时间采取延时读取的策略。
c) 终端应用程序（TA）根据 5.3.7.7 描述的格式解析并进行相应地处理。
d) TA 向卡片进行命令交互必须遵循指令序列执行的流程，否则，SDC 会返回状态字标识“卡片忙”。

5.3.7.9 接口指令

a) 连接智能 SD 卡 SCIF_CONNECT

该命令将指示 SDC 联接内嵌的安全芯片，并将 SDC 的状态从 S1 切换到 S2 状态。请求报文见表 15，参数定义见表 16。

1） 请求报文

表 15 连接智能 SD 卡请求报文

序号	偏移	字节长度	含义	值
1	0	2	SSC	0000
2	2	2	命令码	SCIF_CONNECT
3	4	2	命令长度	01
4	6	1	数据域	PARAMETER
5	7	1	校验字节	LRC

表 16 PARAMETER 定义

8	7	6	5	4	3	2	1	含义
x								访问模式（0：独占模式；1：共享模式）
	0	0	0	0	0	0	0	RFU

2） 响应报文

通讯状态码如果是 SCIF_OK，则应包含 2 个字节的初始 SSC 和可选数据域。连接智能 SD 卡的响应报文见表 17。

表 17 连接智能 SD 卡的响应报文

序号	偏移	字节长度	含义	备注
1	0	2	SSC	0000
2	2	2	通讯状态码	必须
3	4	--	响应数据长度	必须
3	4	--	初始 SSC 及 SDC 特性（SDC 特性定义见表 18）	必须
4	5	1	接口文件个数(HEX 格式)	可选
5	6	1	字节校验和	必须

表 18 SDC 特性定义

8	7	6	5	4	3	2	1	含义
x								1：支持共享模式；0：仅独占模式
	x							RFU
		x						1：支持PPS；0：不支持PPS
			x	x	x	x	x	RFU

b） 请求卡片复位信息 SCIF_ATR

1） 请求报文

复位卡片请求报文家表 19。

表 19 复位卡片请求报文

序号	偏移	字节长度	含义	值
1	0	2	SSC	xx
2	2	2	命令码	SCIF_ATR
3	4	2	命令长度	00
4	6	0	数据域	
5	6	1	校验字节	LRC

2） 响应报文

通讯状态码如果是 SCIF_OK，则应包含安全芯片的上电复位应答信息。复位应答响应报文见表 20。

表 20 复位应答响应报文

序号	偏移	字节长度	含义	值
1	0	2	SSC	SCIF_ATR 请求报文的 SSC
2	2	2	通讯状态码	SCIF_OK
3	4	2	响应数据长度	xx
4	6	--	响应数据	安全芯片的 ATR
5	xx	1	字节校验和	LRC

c） 查询智能 SD 卡信息 SCIF_INFO

1） 请求报文

查询智能 SD 卡信息的请求报文见表 21。

表 21 查询智能 SD 卡信息的请求报文

序号	偏移	字节长度	含义	值
1	0	2	SSC	xx
2	2	2	命令码	SCIF_INFO
3	4	2	命令长度	00
4	6	0	数据域	
5	6	1	校验字节	LRC

2） 响应报文

通讯状态码如果是 SCIF_OK，则应包含智能 SD 卡的版本信息。查询智能 SD 卡的响应报文见表 22。

表 22 查询智能 SD 卡信息响应报文

序号	偏移	字节长度	含义	值
1	0	2	SSC	SCIF_INFO 请求报文的 SSC
2	2	2	通讯状态码	SCIF_OK
3	4	2	响应数据长度	xx
4	6	xx	响应数据	智能 SD 卡的版本信息（见表 23）
5	xx	1	字节校验和	LRC

表 23 智能 SD 卡版本信息格式

序号	偏移	字节长度	含义	存在方式
1	0	2	固定标识：0x0111—智能 SD 卡	必须
2	2	2	协议版本号	必须
3	4	8	产品序列号	必须
4	12	2	支持速率的 Fi 因子	必须
5	14	2	支持速率的 Di 因子	必须
6	16	2	安全单元（SE)的 COS 平台型号信息	必须
7	18	100	保留字段	可选

支持速率的 Fi 因子是如下定义的，在 GB/T16649 协议中定义了 12 种 Fi 传输因子，此字段表明了此智能 SD 卡所支持的 Fi 传输因子，对应关系如表 24。

表 24 Fi 因子的支持

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	含义
RFU	RFU	RFU	RFU	0d	0c	0b	0a	9	6	5	4	3	2	1	0	对应位为 1 就表示支持对应的 Fi 传输因子，为 0 就表示不支持

支持速率的 Di 因子是如下定义的，在 GB/T 16649.3 中定义了 8 种 Di 传输因子，此字段表明了此智能 SD 卡所支持的 Di 传输因子，对应关系如表 25：

表 25 Di 因子的支持

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	含义

RFU	RFU	RFU	RFU	RFU	RFU	RFU	RFU	9	8	6	5	4	3	2	1	对应位为 1 就表示支持对应的 Di 传输因子，为 0 就表示不支持

如果在命令 SCIF_INFO 的响应报文中取得这两个字段的内容是 0X02410025,那么根据上表就可以得知此版本的智能 SD 卡可以支持的传输速率有：Fi= 0b,06,01;Di=06,03,01;一共 3*3=9 种组合的速率。

安全单元（SE)的 COS 平台型号信息的定义如表 26 所示。

表 26 安全单元（SE)的 COS 平台型号信息定义

B8	B7	B6	B5	B4	B3	B2	B1	含义
RFU						x	x	安全单元（SE)的 COS 平台型号
						0	0	Native
						0	1	JavaCard+Global Platform
						1	0	RFU
						1	1	RFU

d) 请求 PPS 交换 SCIF_PPS

1) 请求报文

PPS 交换请求报文见表 27。

表 27 PPS 交换请求报文

序号	偏移	字节长度	含义	值
1	0	2	SSC	xx
2	2	2	命令码	SCIF_PPS
3	4	2	命令长度	01
4	6	1	数据域	Rate
5	7	1	校验字节	LRC

Rate 表示 SDC 和安全芯片在数据传输时的波特率参数，用一个字节来定义它。SDC 和安全芯片之间的数据传输可以采取不同的速率,不要求智能 SD 卡必需支持能够采用不同速率和安全芯片进行交互，但是如果支持这个特性，就必需提供接口让 TA 可以通过 PPS 请求调整传输速率。

Rate 参数可以分为两个半字节来定义它，具体定义如下：

Rate = FI | DI

FI 这半字节（二进制表示）的取值范围是：0000，0001，0010，0011，0100，0101，0110，1001，1010，1011，1100，1101，而 0111，1110，1111 这 3 个是 RFU 的值，未定义。

DI 这半字节（二进制表示）的取值范围是：0001，0010，0011，0100，0101，0110，1000，1001，其余的取值都是 RFU 的值，未做定义。

Rate 的取值可以是上面取值范围内的 FI 和 DI 的任意组合，但是并不要求智能 SD 卡支持上述的所有速率，TA 在进行 PPS 请求的时候必需参阅智能 SD 卡的手册，了解智能 SD 卡可以支持哪些传输参数。

2) 响应报文

通讯状态码如果是 SCIF_OK,则响应报文中应该包含安全芯片 PPS 响应的信息。PPS 交换响应报文见表 28。

表 28 PPS 交换响应报文

序号	偏移	字节长度	含义	值
1	0	2	SSC	SCIF_PPS 请求报文的 SSC
2	2	2	通讯状态码	SCIF_OK
3	4	2	响应数据长度	xx

4	6	xx	响应数据	安全芯片的 PPS 响应的值
5	xx	1	字节校验和	LRC

TA 应该能够根据 GB/T 16649 中的规定解析安全芯片返回的 PPS 响应，判断此次 PPS 请求是否成功。

e) 转发 APDU SCIF_APDU

1) 请求报文

转发 APDU 请求报文见表 29。

表 29 转发 APDU 请求报文

序号	偏移	字节长度	含义	值
1	0	2	SSC	xx
2	2	2	命令码	SCIF_APDU
3	4	2	命令长度	xx
4	6	xx	数据域	APDU
5	xx	1	校验字节	LRC

2) 响应报文

如果通讯状态码是 SCIF_OK，则响应报文中应该包含命令状态码和安全芯片回复的数据信息。转发 APDU 响应报文见表 30。

表 30 转发 APDU 响应报文

序号	偏移	字节长度	含义	值
1	0	2	SSC	SCIF_APDU 请求报文的 SSC
2	2	2	通讯状态码	SCIF_OK
3	4	2	响应数据长度	xx
4	6	xx	响应数据	
5	xx	1	字节校验和	LRC

在响应数据中命令状态码在响应数据域的最后两个字节。

f) 断开智能卡 SCIF_DISCONNECT

该命令将指示 SDC 断开内嵌的安全芯片，并将 SDC 和安全芯片恢复到初始状态，即将 SDC 的状态从 S3 切换到 S1 状态，同时销毁内部的会话标识，清掉内部发送序列计数器的会话流水号。

1) 请求报文

断开连接请求报文见表 31。

表 31 断开连接请求报文

序号	偏移	字节长度	含义	值
1	0	2	SSC	xxxx
2	2	2	命令码	SCIF_DISCONNECT
3	4	2	命令长度	00
4	6	0	数据域	
5	6	1	校验字节	LRC

2) 响应报文

断开连接响应报文见表 32。

表 32 断开连接响应报文

序号	偏移	字节长度	含义	值
1	0	2	SSC	SCIF_DISCONNECT 请求报文的 SSC
2	2	2	通讯状态码	SCIF_OK
3	4	2	响应数据长度	00
4	6	xx	响应数据	

5	xx	1	字节校验和	LRC

5.4 双界面(U)SIM卡

5.4.1 物理特性

双界面(U)SIM卡的物理特性应符合GB/T 16649.1的要求。

5.4.2 接触通道的电气特性和传输协议

双界面(U)SIM卡的接触通道的接口电气特性和传输协议应符合GB/T 16649.2和GB/T 16649.3的要求。

5.4.3 非接触通道的电气特性和传输协议

非接触通道的电气特性和传输协议参见JR/T XXXXX 中国金融移动支付 非接触式接口规范。

5.4.4 安全单元逻辑结构

双界面(U)SIM 卡安全单元包括接触通道和非接触通道，接触通道和非接触通道应具有并发处理能力，并互不影响。

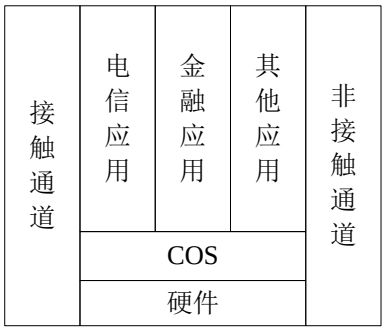

图 22 双界面(U)SIM卡逻辑结构图

5.4.5 双界面(U)SIM卡扩展接口定义

5.4.5.1 硬件结构

实现双界面方案的移动支付终端部件至少包含双界面(U)SIM、天线等模块，如图23所示：

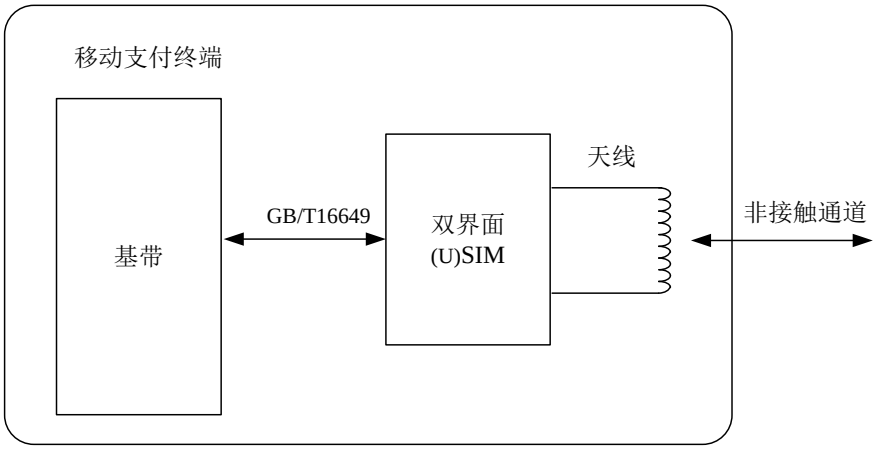

图 23 基于双界面(U)SIM卡的移动支付方案结构图

5.4.5.2 电源管理

当移动终端开机时，或关机但电池仍能通过电源管理系统正常提供电源能量时，双界面(U)SIM可使用移动终端的电池作为电源能量；当移动终端的电池被取下时，或电池无法通过电源管理系统正常提供电源能量时，双界面(U)SIM应选择使用其通过天线线圈从受理终端的工作场中感应得到的电源能量，但此功能不做强制要求。

在双界面(U)SIM获得正常工作所需的电源能量的情况下，应能正常执行金融应用。

5.4.5.3 双界面(U)SIM卡尺寸

(U)SIM 卡的触点尺寸应符合GB/T 16649.2的要求。(U)SIM卡的外形尺寸应符合ETSI 102 221的要求。

5.4.5.4 双界面(U)SIM卡触点定义

双界面(U)SIM卡是基于CLF和安全单元（SE)集成于一体的安全载体，包括C1、C2、C3、C4、C5、C6、C7、C8共8个引脚，如图24所示。其中C4、C8引脚可作为非接触天线接口，C6引脚暂不作定义，其余5个引脚应符合JR/T 0025.3的规定。

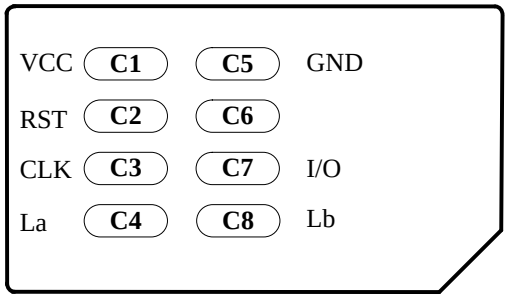

图 24 双界面(U)SIM卡触点

双界面(U)SIM卡触点定义如表33所示：

表 33 双界面(U)SIM卡触点定义

管脚号	名称	类型	描述
C1	VCC	P	电源电压
C2	RST	I/O	复位
C3	CLK	I/O	时钟
C4	La	I/O	非接触天线接口
C5	GND	I	地
C6	RFU		保留
C7	I/O	I/O	串行数据输入/输出
C8	Lb	I/O	非接触天线接口