



# 中华人民共和国通信行业标准

YD/T 2774-2014

---

## 手机支付 基于 2.45GHz RCC(限域通信)技术的 智能卡技术要求

Mobile payment technical requirements for intellegent card based  
on 2.45GHz RCC(Range Controlled Communication)technology

2014-12-24 发布

2014-12-24 实施

---

中华人民共和国工业和信息化部 发布



目 次

前 言.....III

1 范围.....1

2 规范性引用文件.....1

3 术语、定义和缩略语.....1

    3.1 术语和定义.....1

    3.2 缩略语.....2

4 基于 2.45GHz RCC(限域通信)技术的智能卡总体技术要求.....2

    4.1 概述.....2

    4.2 硬件架构.....3

    4.3 软件架构.....4

5 物理特性.....5

    5.1 一般物理特性.....5

    5.2 格式和布局.....5

6 电气特性.....7

    6.1 电信号描述.....7

    6.2 电压和电流.....7

7 通信接口特性.....8

    7.1 接触式通信接口.....8

    7.2 非接触式通信接口.....8

    7.3 接口数据并发处理.....8

    7.4 多应用支持.....8

8 CIOS/COS 架构接口管理.....9

    8.1 CIOS 接口概述.....9

    8.2 APDU 接口.....9

    8.3 TPDU 接口.....9

9 安全模块技术要求.....10

    9.1 硬件要求.....10

    9.2 芯片硬件安全要求.....10

    9.3 CIOS/COS 软件安全要求.....10

    9.4 数据安全要求.....10

    9.5 访问控制安全要求.....10

    9.6 交易保护机制(Transaction).....10

    9.7 多应用管理协议要求.....10

YD/T 2774-2014

附录 A（规范性附录） CIOS APDU 接口.....11

附录 B（规范性附录） CIOS TPDU 接口.....17

附录 C（资料性附录） CIOS/COS 技术特性.....20

附录 D（资料性附录） COS 开发及接口使用范例.....21



## 前 言

本标准按照GB/T 1.1-2009给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准是手机支付系列标准之一。该系列标准的名称预计如下：

1. 手机支付 术语和定义
2. 手机支付 总体技术要求
3. 手机支付 基于13.56MHz近场通信技术的手机终端技术要求
4. 手机支付 基于13.56MHz近场通信技术的智能卡和内置安全模块技术要求
5. 手机支付 基于2.45GHz RCC（限域通信）技术的智能卡技术要求
6. 手机支付 基于13.56MHz近场通信技术的非接触式销售点终端技术要求
7. 手机支付 基于2.45GHz RCC（限域通信）技术的非接触式读写器终端技术要求
8. 手机支付 基于13.56MHz和2.45GHz双频的非接销售点终端技术要求
9. 手机支付 基于13.56MHz 近场通信技术的非接触射频接口技术要求
10. 手机支付 基于2.45GHz RCC（限域通信）技术的非接触射频接口技术要求
11. 手机支付 智能卡和内置安全模块安全技术要求
12. 手机支付 移动终端安全技术要求
13. 手机支付 多应用管理协议技术要求
14. 手机支付 基于13.56MHz近场通信技术的手机终端测试方法
15. 手机支付 基于13.56MHz近场通信技术的智能卡和内置安全模块测试方法
16. 手机支付 基于2.45GHz RCC（限域通信）技术的智能卡测试方法
17. 手机支付 基于13.56MHz近场通信技术的非接触式销售点终端测试方法
18. 手机支付 基于2.45GHz RCC（限域通信）技术的非接触式读写器终端测试方法
19. 手机支付 基于13.56MHz和2.45GHz的双频非接销售点终端测试方法
20. 手机支付 基于13.56MHz 的非接触射频接口测试方法
21. 手机支付 基于2.45GHz RCC（限域通信）技术的非接触射频接口测试方法
22. 手机支付 智能卡和内置安全模块安全测试方法
23. 手机支付 移动终端安全测试方法
24. 手机支付 多应用管理协议测试方法

本标准由中国通信标准化协会提出并归口。

本标准起草单位：工业和信息化部电信研究院、中国电信集团公司、中国移动通信集团公司、中国联通网络通信集团公司。

本标准主要起草人：贺 倩、袁 琦、杨贤伟、王 逖、姜志峰、高 玲、葛 欣、张 强、李铭轩。

手机支付

基于 2.45GHz RCC（限域通信）技术的智能卡技术要求

1 范围

本标准规定了基于 2.45GHz RCC（限域通信）技术的智能卡技术要求，包括智能卡软硬件技术架构、物理特性、电气特性、通信接口、多应用支持、安全模块要求以及应用开发接口等内容。

本标准适用于支持基于2.45GHz RCC（限域通信）技术的智能卡。

2 规范性引用文件

下列文件对于本标准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标准。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本标准。

YD/T 1762.1-2011	TD-SCDMA/WCDMA 数字蜂窝移动通信网 通用集成电路卡 (UICC)与终端间Cu接口技术要求 第1部分：物理、电气和逻辑特性
YD/T 1762.2-2011	TD-SCDMA/WCDMA数字蜂窝移动通信网 通用集成电路卡(UICC)与终端间Cu接口技术要求 第2部分：通用用户识别模块（USIM）应用特性
ETSI TS 102 221 V8.3.0	智能卡 UICC终端接口 物理和逻辑特性
ISO/IEC 7816-1	识别卡 带触点的集成电路卡 第1部分：物理特性
ISO/IEC 7816-2	识别卡 集成电路卡 第2部分:带触点的卡 触点的尺寸和定位
ISO/IEC 7816-3	识别卡.集成电路卡 第3部分:带触点的卡 电接口和传输协议

3 术语、定义和缩略语

3.1 术语和定义

3.1.1

RF-(U)SIM

基于2.45GHz RCC（限域通信）技术的(U)SIM卡。

3.1.2

卡片IO管理系统 Card IO Management System

卡片中间件软件模块，实现RF射频通道和7816接口的底层硬件接口管理和数据并发处理，并为上层COS提供API接口管理。

3.1.3

7816接口 7816 Interface

符合ISO/IEC 7816协议规范的接口模块，用于卡片和移动终端设备之间进行连接，或者用于智能卡内部安全模块和电信模块之间进行连接。

3.1.4

HOOK接口 HOOK Interface

由CIOS调用、COS实现并可监控或改变执行结果的API接口。

3.1.5

安全模块 Security Module

采用双模块结构实现的2.45GHz RF-(U)SIM卡上的一个功能模块，该模块用于实现2.45GHz射频通信处理以及安全应用功能。

3.1.6

电信模块 Telecommunication Module

采用双模块结构实现的2.45GHz RF-(U)SIM卡上的一个功能模块，该模块用于实现移动通信应用功能。

3.1.7

安全/电信模块 Security/Telecommunication Module

采用单模块结构实现的2.45GHz RF-(U)SIM卡上的一个功能模块，该模块既用于实现2.45GHz射频通信处理以及安全应用功能，同时又用于实现移动通信应用功能。

3.2 缩略语

APDU	Application Protocol Data Unit	应用协议数据单元
API	Application Programming Interface	应用程序编程接口
CIOS	Card IO Management System	卡片IO管理系统
DME	Dual Module Encapsulation	双模块结构
GSM	Global System for Mobile communications	全球移动通信系统
ISM	Industrial Scientific Medical	工业、科学和医疗
ISO	International Organization for Standardization	国际标准化组织
RF	Radio Frequency	射频
SME	Single Module Encapsulation	单模块结构
TPDU	Transport Protocol Data Unit	传输协议数据单元
(U)SIM	(Universal)Subscriber Identity Module	用户识别模块

4 基于 2.45GHz RCC（限域通信）技术的智能卡总体技术要求

4.1 概述

本标准所述限域通信系统由2.45GHz RF-(U)SIM卡和2.45GHz RF-(U)SIM读写器组成，在卡和读写器之间采用磁通道和2.45GHz射频双通道机制，将磁通道和2.45G射频通道进行绑定，共同完成射频通信功能。磁通道利用准静态磁场，以耦合方式完成可靠距离控制；射频通道采用2.45GHz工业、科学和医疗（ISM）频段，以电磁场发射接收方式完成高速数据交换。协议会话层采用密码技术对射频通道交换的应用协议数据单元（APDU）数据进行加密传输，加解密操作对上层应用完全透明。

本标准使用(U)SIM卡作为载体，采用上述准静态磁与射频双通道通信方法，在保证原有(U)SIM通信的条件下实现基于2.45GHz限域通信技术的无线通信，使得一张(U)SIM卡可同时具有射频通信功能和传统电信功能，从而构成2.45GHz RF-(U)SIM卡。RF-(U)SIM卡射频通信具体要求符合YD/T 2772《手机支付 基于2.45GHz RCC（限域通信）技术的非接触射频接口技术要求》规定。



## 4.2 硬件架构

### 4.2.1 架构概述

2.45GHz RF-(U)SIM在硬件架构上可分为单模块结构（SME）和双模块结构（DME）。采用SME结构实现的RF-(U)SIM卡和采用DME结构实现的RF-(U)SIM卡在功能和应用范围等方面没有任何区别，只是产品实现方式的不同。在DME结构下，采用一个安全模块实现2.45GHz射频通信处理以及安全应用功能，采用一个电信模块实现移动通信应用功能；在SME结构下，采用一个安全/电信模块同时实现2.45GHz射频通信处理、安全应用功能以及移动通信应用功能。

### 4.2.2 单模块结构（SME）

单模块结构（SME）主要由安全/电信模块、射频接口和7816接口组成。SME将安全应用功能和传统电信应用功能集成在同一个“安全/电信”模块内。

单模块硬件结构如图1所示。

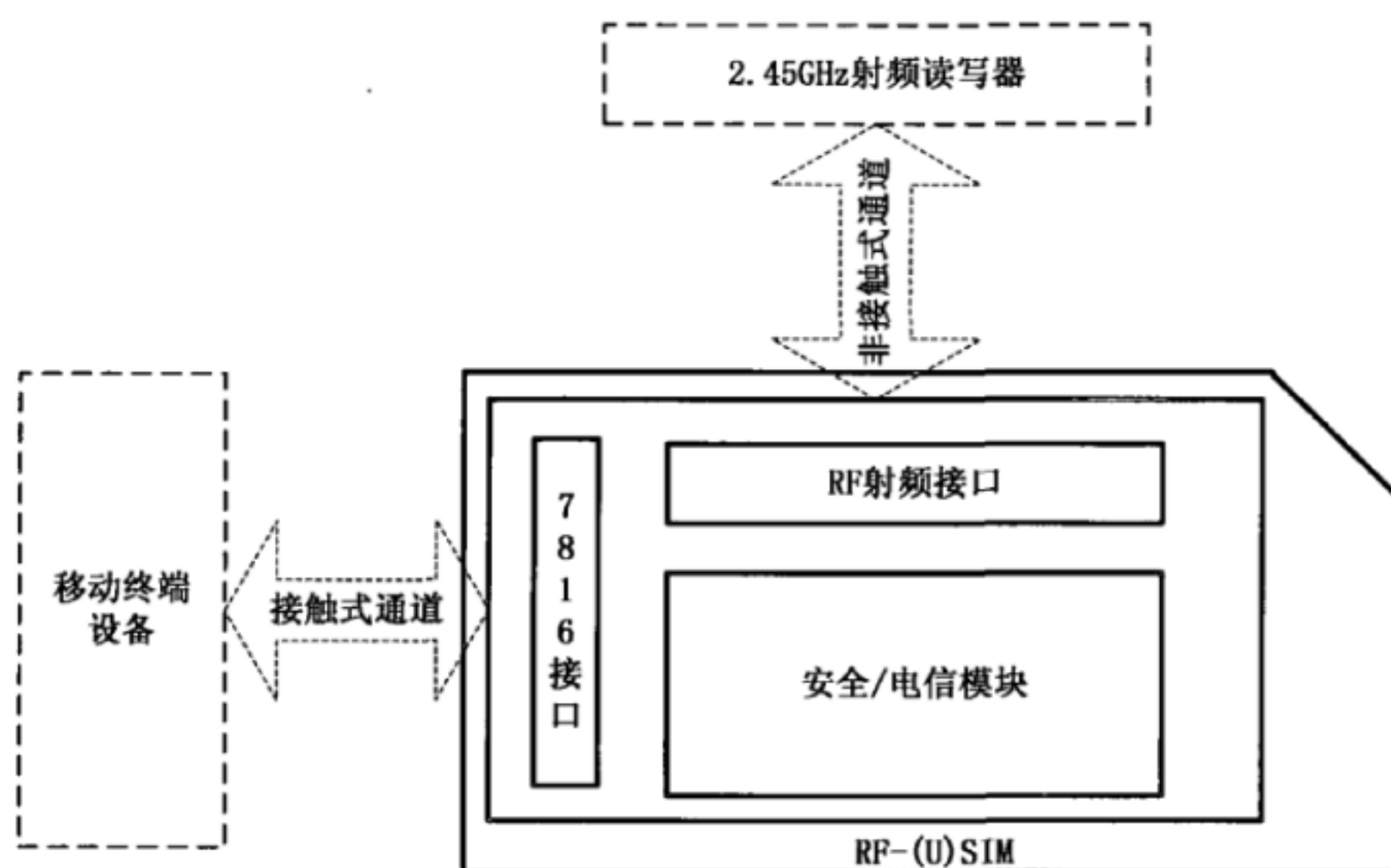


图1 RF-(U)SIM 单模块结构示意图

其中，RF射频接口主要用于非接触通信中，处理2.45GHz射频和磁通道的数据发送/接收；7816接口用于移动终端设备与RF-(U)SIM间的通信；安全/电信模块实现对2.45GHz非接触通道的通信控制、安全应用以及传统移动通信应用功能。

### 4.2.3 双模块结构（DME）

双模块结构（DME）主要由安全模块、电信模块、射频接口和两个7816接口组成。在双模块结构中，由安全模块和电信模块两个独立的功能模块分别完成2.45GHz非接触通道的通信控制、安全应用和传统移动通信功能。

双模块硬件结构如图2所示。

其中，RF射频接口、7816接口与SME结构相同，新增7816接口用于安全模块与电信模块之间的连接；安全模块实现对2.45G非接触通道的通信控制、安全应用以及移动终端设备与电信模块之间的数据转发；卡内独立的电信模块用于实现传统电信应用功能。

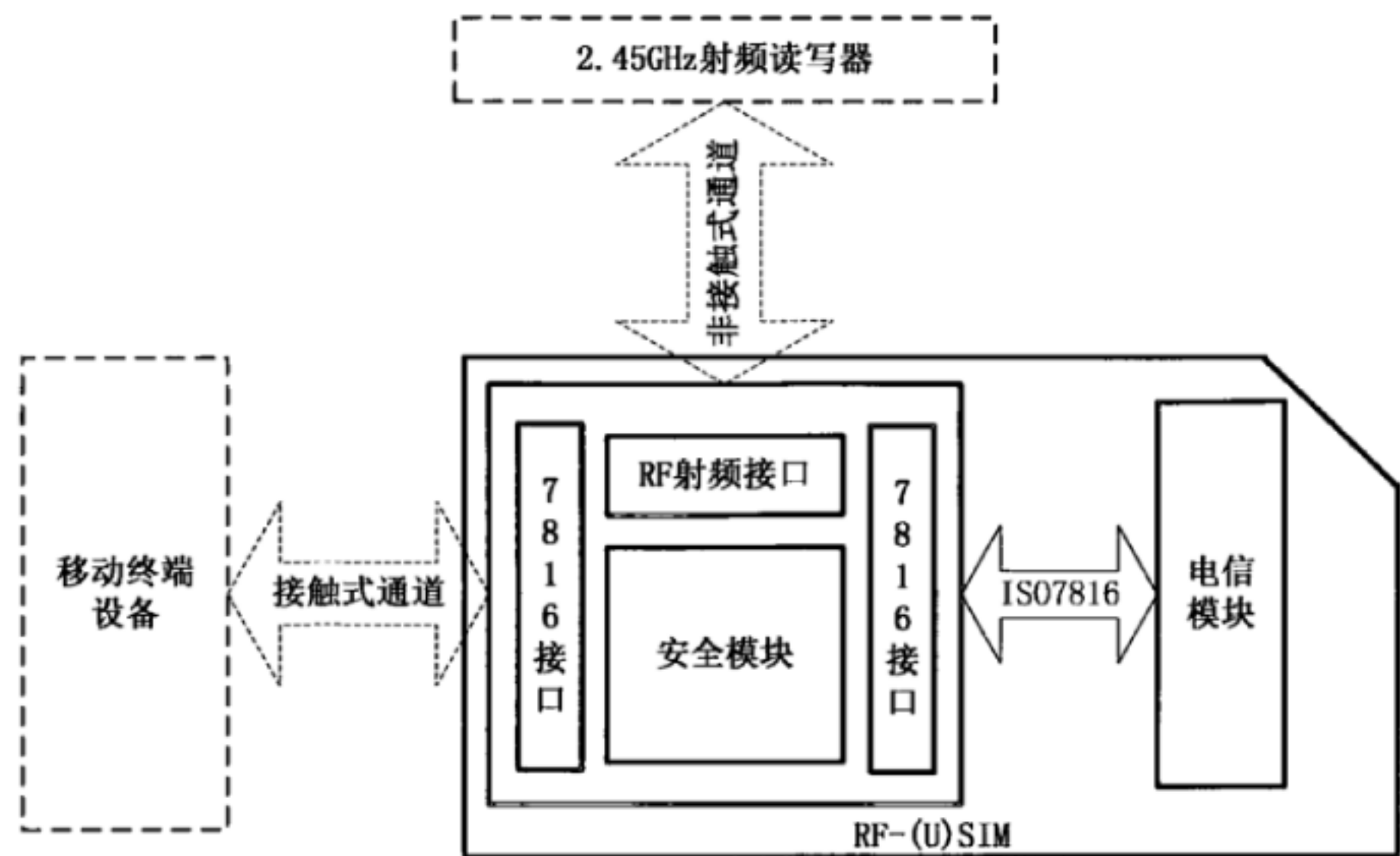


图2 RF-(U)SIM 双模块结构示意图

4.3 软件架构

软件架构示意如图3所示。

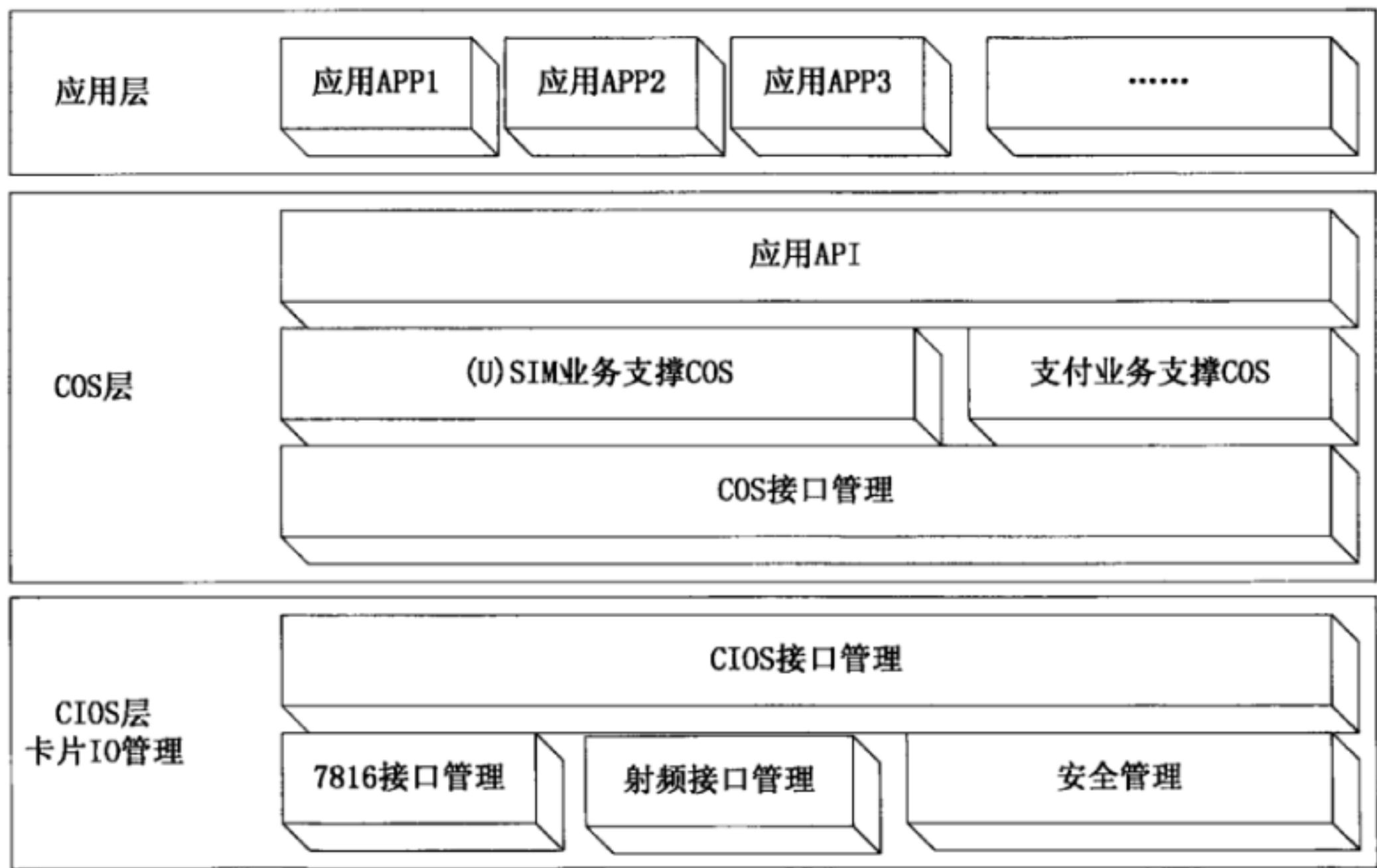


图3 RF-(U)SIM 软件架构示意

RF-(U)SIM 卡软件架构主要分为三层：

(1) CIOS 层

CIOS层实现智能卡IO管理，包含以下基本功能：

- 7816 接口管理。控制 7816 硬件接口，实现 RF-(U)SIM 卡与移动终端设备之间或者 RF-(U)SIM 卡内部安全模块与电信模块之间的数据通信。
- RF 射频接口管理。控制 RF 射频硬件接口，实现 RF-(U)SIM 卡与读写器之间的非接触式近距离数据通信。

- 安全管理。实现 RF-(U)SIM 卡内不同应用之间的隔离和安全访问控制。
- CIOS 接口管理。实现 7816 接口与 RF 射频接口两个通信接口的数据并行处理；向 COS 层提供 CIOS API 接口。

## (2) COS 层

COS层实现卡片操作及应用支撑管理，包含以下基本功能：

- COS 接口管理。接收 CIOS 层的数据，供 COS 和应用层处理，并回传处理结果给 CIOS 层。
- (U)SIM 业务支撑 COS。实现与电信业务相关的文件管理和数据处理，为电信应用提供业务基础支撑。
- 支付业务支撑 COS。实现与支付应用相关的文件管理和数据处理，为支付应用提供业务基础支撑。
- 应用 API。为应用层提供 API 处理接口，实现应用层对 COS 层业务功能模块的调用。

## (3) 应用层

应用层实现基于接触式和非接触式通信接口的各种业务功能。

# 5 物理特性

## 5.1 一般物理特性

RF-(U)SIM卡的一般物理特性应符合ISO/IEC 7816-1《识别卡 带触点的集成电路卡 第1部分：物理特性》第4章要求。

## 5.2 格式和布局

### 5.2.1 最小接触面积

RF-(U)SIM卡触点最小接触面积符合ISO/IEC 7816-2《识别卡 集成电路卡 第2部分：带触点的卡 触点的尺寸和定位》第3章规定。

### 5.2.2 PLUG-IN 卡几何尺寸

RF-(U)SIM采用PLUG-IN方式，并配以卡基使用以便于发行及运输。RF-(U)SIM卡外形尺寸以及在卡基上的位置符合YD/T1762.1-2011《TD-SCDMA/WCDMA 数字蜂窝移动通信网 通用集成电路卡(UICC)与终端间Cu接口技术要求 第1部分：物理、电气和逻辑特性》第4.3节规定。

### 5.2.3 RF-MiniSIM 卡及卡基几何尺寸

RF-MiniSIM卡及卡基尺寸符合YD/T1762.1-2011《TD-SCDMA/WCDMA 数字蜂窝移动通信网 通用集成电路卡(UICC)与终端间Cu接口技术要求 第1部分：物理、电气和逻辑特性》第4.4节规定。

### 5.2.4 RF-NanoSIM 卡及卡基几何尺寸

RF-NanoSIM卡尺寸如图4所示。

RF-NanoSIM卡尺寸如下：

- 矩形长度：(12.3±0.1) mm。
- 矩形宽度：(8.8±0.1) mm。
- 卡的厚度：(0.70+0.16/-0.1) mm。

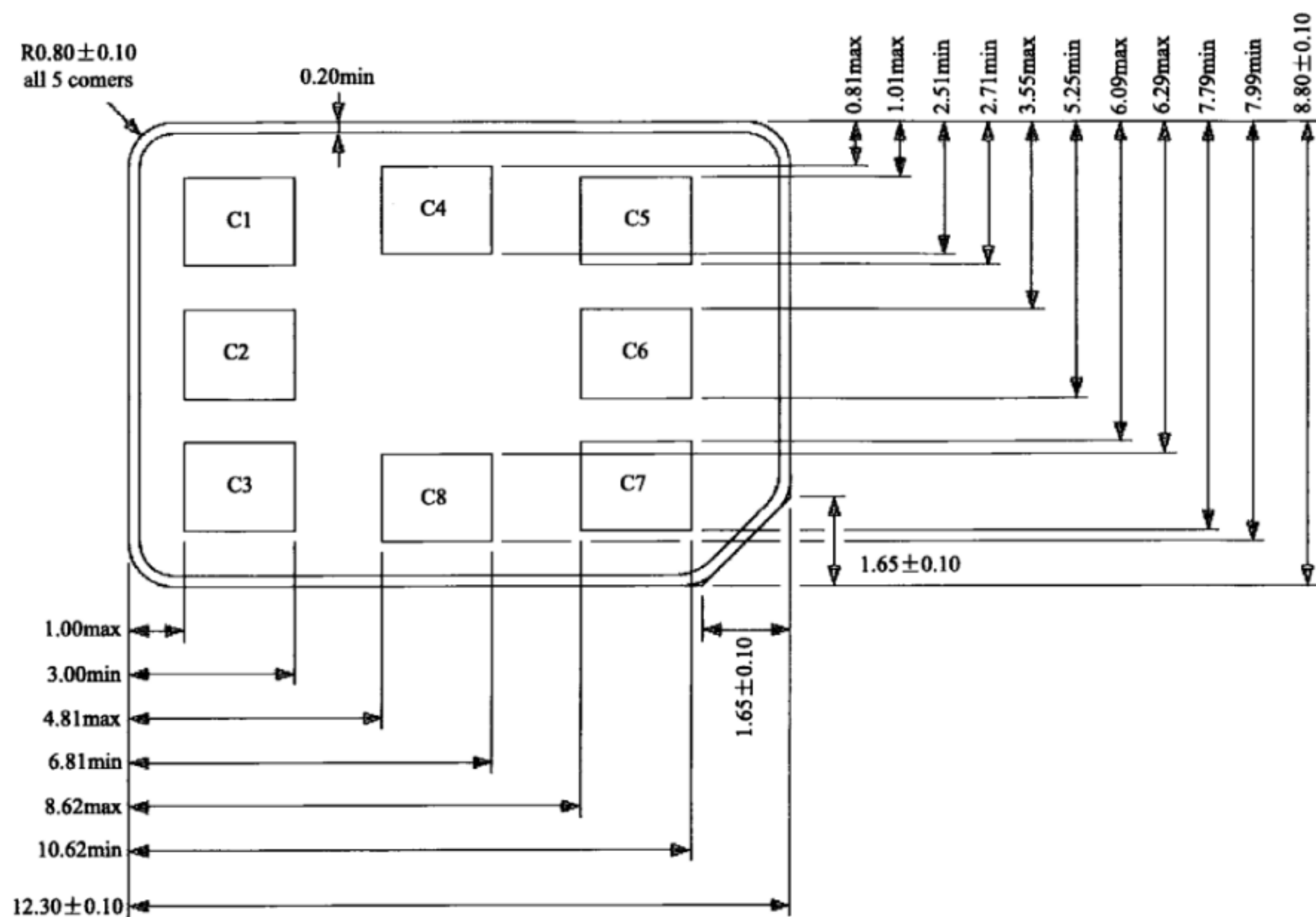


图4 RF-NanoSIM 卡尺寸

RF-NanoSIM卡卡基尺寸如图5所示。

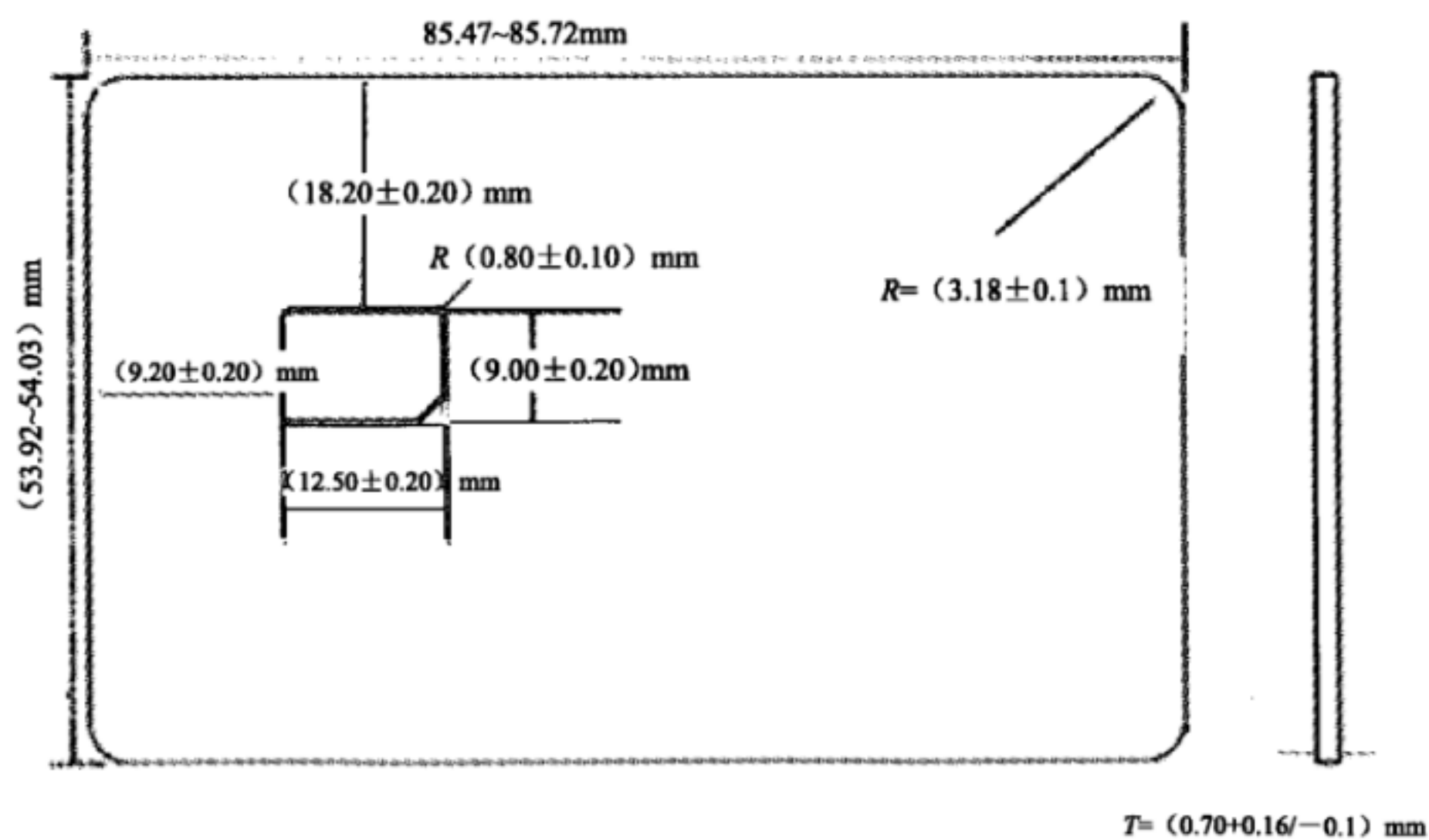


图5 RF-NanoSIM 卡卡基尺寸

RF-NanoSIM卡基尺寸如下:

- 矩形长度: 85.47~85.72mm (缺角为1.78mm±0.1mm的等腰三角形)。
- 矩形宽度: 53.92~54.03mm。
- 厚度: 0.70+0.16/-0.1mm。



- 卡槽尺寸：长 $12.50\pm0.20\text{mm}$ ，宽 $9.00\pm0.20\text{mm}$ 。
- 卡槽左缘与卡基左缘距离： $9.20\pm0.20\text{mm}$ 。
- 卡槽上缘与卡基上缘距离： $18.20\pm0.20\text{mm}$ 。
- 卡槽R角尺寸：5个， $R0.8\pm0.1\text{mm}$ 。

5.2.5 触点分配

RF-(U)SIM卡共有8个触点，触点分布符合ISO/IEC 7816-2《识别卡 集成电路卡 第2部分：带触点的卡 触点的尺寸和定位》第4章规定。

6 电气特性

6.1 电信号描述

RF-(U)SIM卡使用C1、C2、C3、C5、C6、C7共6个触点，触点对应的电信号符合ISO/IEC 7816-3《识别卡.集成电路卡 第3部分：带触点的卡 电接口和传输协议》第5章规定。

6.2 电压和电流

6.2.1 电压限制

卡电压限制符合ETSI TS 102 221 V8.3.0《智能卡 UICC终端接口 物理和逻辑特性》第5章规定。

6.2.2 正常条件下电流限制

在正常的操作（包含7816时钟停止后射频仍然工作）条件下，RF-(U)SIM卡的电流消耗不得超过规定限度。卡电流限制符合ETSI TS 102 221 V8.3.0《智能卡 UICC终端接口 物理和逻辑特性》第6.2.3节表格6.3中对于智能卡在会话期间最大电流消耗的限制要求。卡产生的尖峰电流符合ETSI TS 102 221 V8.3.0《智能卡 UICC终端接口 物理和逻辑特性》第5章对尖峰电流的限制要求。

6.2.3 空闲电流的限制

在空闲条件下RF-(U)SIM卡的电流消耗不得超过规定限度（见表1）。

其中，空闲条件指接触式接口与非接触式接口同时处于空闲状态。

表1 空闲模式下的电流消耗

卡类型	最大电流 $I_{\text{max}}$ 空闲状态下，时钟频率1Mhz (单位：uA)	试验期间 $V_{\text{cc}}$ 上的最大电压 $V_{\text{ccmax}}$ (单位：V)
5V	800	5.5
3V	800	3.3
1.8V	800	1.98

6.2.4 空闲模式全频率下的电流限制

在空闲模式全频率下RF-(U)SIM卡的电流消耗不得超过规定限度（见表2）。

其中，空闲模式全频率指接触式接口处于空闲模式全频率状态，同时非接触式接口处于空闲状态。

表2 空闲模式全频率下的电流消耗

卡类型	空闲状态下的 $I_{\text{max}}$ (平均值) (单位：uA)	空闲模式下的最大CLK频率 $f_{\text{max}}$ (单位：MHz)	试验时 $V_{\text{cc}}$ 上的最大电压 $V_{\text{ccmax}}$ (单位：V)
5V	1000	5	5.5
3V	1000	4	3.3
1.8V	1000	4	1.98

6.2.5 时钟停止模式的电流限制

在时钟停止条件下RF-(U)SIM卡的电流消耗不得超过规定限度（见表3）。  
其中，时钟停止模式指接触式接口时钟停止，同时非接触式接口处于空闲状态。

表3 7816-CLK 时钟停止模式下的电流消耗

卡类型	时钟停模式下最大电流 $I_{\max}$ （平均值） （单位：uA）	试验期间 $V_{cc}$ 上的最大电压 $V_{ccmax}$ （单位：V）
5V	800	5.5
3V	800	3.3
1.8V	800	1.98

6.2.6 I/O、CLK、RST 的电压和电流特性

RF-(U)SIM卡的I/O、CLK、RST等其他电信号特性，符合YD/T 1762.1-2011《TD-SCDMA/WCDMA 数字蜂窝移动通信网 通用集成电路卡(UICC)与终端间Cu接口技术要求 第1部分：物理、电气和逻辑特性》规定和ISO/IEC 7816-3《识别卡.集成电路卡 第3部分:带触点的卡 电接口和传输协议》规定。

7 通信接口特性

7.1 接触式通信接口

接触式通道采用7816串行通信接口，其物理特性和通信协议符合ISO/IEC 7816-3《识别卡.集成电路卡 第3部分：带触点的卡 电接口和传输协议》规定。7816接口必须支持T=0通信协议。

7.2 非接触式通信接口

非接触式通道采用2.45G射频和磁场进行通信，其物理特性和通信协议符合YD/T 2772《手机支付 基于2.45GHz RCC（限域通信）技术的非接触射频接口技术要求》规定。

7.3 接口数据并发处理

7.3.1 接口数据并发

并发处理是指当RF-(U)SIM卡通过接触式接口通信的状态下，同时接收并响应非接触式接口数据，以及当通过非接触式接口通信，同时接收并响应到接触式接口数据的处理。

7.3.2 并发处理要求

本标准要求RF-(U)SIM卡支持基于非接触式接口和接触式接口数据的并发处理。  
RF-(U)SIM卡要求可以同时处理来自非接触式接口和接触式接口的数据。RF-(U)SIM卡应保证非接触式接口数据传输和接触式接口数据传输的互不影响。

7.4 多应用支持

7.4.1 多应用技术要求

RF-(U)SIM卡允许多个应用共存，在COS层多应用并存的情况下，应保证各种应用交叉处理的可靠性。  
同一通信接口的不同应用处理由相关业务规范定义，同一通信接口的不同逻辑通道的数据处理由相关业务规范定义，均不在本标准要求范围。

7.4.2 多应用安全性

RF-(U)SIM卡两个通信接口的应用应该运行在各自独立的系统空间内，有良好的实时响应和数据安全性。  
RF-(U)SIM卡应保证卡上各应用间数据相互隔离，未经应用授权均无法获取其私有和秘密数据。  
RF-(U)SIM卡保证卡上应用的下载与删除不影响到其他应用。

8 CIOS/COS 架构接口管理

8.1 CIOS 接口概述

在基于CIOS/COS的固件架构中，CIOS层提供多种API接口，供COS层和应用层调用。  
CIOS在接触式通道上提供的接口分为APDU接口和TPDU接口。

8.2 APDU 接口

CIOS提供的APDU接口分为系统接口和HOOK接口。  
其中，CIOS系统接口是指由COS调用、由CIOS提供功能的接口函数，用于获取和操作系统资源等。  
HOOK接口则是由CIOS调用、由COS实现的接口函数，用于监控或改变指令执行结果。

表4为CIOS APDU接口列表。

表4 APDU 接口列表

函数名称	说明
系统接口	
Set_Boot	重新进入COS下载状态
Get_Ver	获取CIOS版本号
RF_Start	打开/关闭RF射频接口
RF_Send	RF射频接口数据发送
RF_Status	获取RF射频接口通道连接状态
Get_ICID	获取卡片唯一标识
SIM_APDU_Transmit	实现RF射频接口模块与电信模块之间的数据转发 (本函数仅适用于双模块结构)
HOOK接口	
COSFun_Param_Init	COS 全局变量、文件系统初始化
RF_APDUData_Process_Function	用于将RF射频接口接收到的数据上传给COS进行处理，并获取处理结果，然后通过RF射频接口进行发送
Find_7816APDU_Instruction	查找COS支持的指令列表，用于判断7816接口模块接收到的指令，是否为COS所需要处理的指令
Get_7816APDU_Instruction_Description	获取指令属性，并根据指令属性决定是否修改指令数据和/或改变指令传送方向
Monitor_IncomingAPDU_Instruction	7816接口命令监控，对于Lc类型的指令，由COS决定是否进行指令数据的修改、或改变指令的传输方向
Check_OutgoingData_Hook	监控电信模块指令返回的执行结果，并由COS决定是否对执行结果进行处理。 (本函数仅适用于双模块结构)
Exec_COS_Instruction	执行7816接口命令并返回执行结果
Cos_process_instruction_not_in_table	对于COS不识别的指令，返回处理结果 (本函数仅适用于单模块结构)

8.3 TPDU 接口

TPDU接口用于7816传输层协议数据单元（TPDU）的接收和发送。  
CIOS提供的TPDU接口分为系统接口和HOOK接口，详见表5。



表5 TPDU 接口列表

函数名称	说明
系统接口	
ISO7816VMInit	初始化7816接口数据接收环境
7816S_RecvByte	7816接口接收移动终端数据
7816S_SendByte	7816接口向移动终端发送数据
GetSIMResponse	COS 调用该接口获取电信模块的应答数据，即该函数向电信模块发送指令数据，并接收电信模块指令执行的响应数据（本函数仅适用于双模块结构）
CosBridge	将TPDU接口数据转发至APDU接口进行处理
HOOK接口	
ISO7816_VM	COS层7816接口指令处理入口

9 安全模块的技术要求

9.1 硬件要求

安全模块的硬件结构如图2所示，安全模块通过7816接口与电信模块和手机终端通信，通过射频接口与射频读写器通信。

9.2 硬件安全要求

RF-(U)SIM卡安全模块涉及支付应用敏感数据的存储和处理，整体安全能力应达到EAL4+以上。  
安全模块硬件安全性应符合YD/T 2501-2013 《手机支付 智能卡和内置安全模块安全技术要求》第5章的规定。

9.3 CIOS/COS 软件安全要求

安全模块CIOS/COS软件安全性应符合YD/T 2501-2013 《手机支付 智能卡和内置安全模块安全技术要求》第6章的规定。

9.4 数据安全要求

RF-(U)SIM卡数据存储、传输以及恢复应符合YD/T 2501-2013 《手机支付 智能卡和内置安全模块安全技术要求》第7章规定。

9.5 访问控制安全要求

RF-(U)SIM卡应支持的访问控制安全要求应符合YD/T 2501-2013 《手机支付 智能卡和内置安全模块安全技术要求》第8章规定。

9.6 交易保护机制(Transaction)

安全模块应具有保护交易数据更新的逻辑机制。交易保护必须是原子性操作，即要么所有的数据都被更新，要么都不更新。安全模块需支持原子性交易保护操作，应用数据在更新失败时可以恢复成原来的数据。交易保护机制可以防止在一个事务操作中，由于断电或者程序上的错误导致的只有一部分数据被更新的情况出现。

9.7 多应用管理协议要求

安全模块中多应用管理协议要求具体参见《手机支付 多应用管理协议技术要求》规定。

附 录 A  
(规范性附录)  
CIOS APDU 接口

A.1 CIOS接口

A.1.1 Set\_Boot

函数原型	void Set_Boot (void)
功能说明	使能COS重新下载状态，用于更新COS程序
函数参数	无
返回值	无
相关参考	无
注意事项	COS根据需要控制下载权限

A.1.2 Get\_Ver

函数原型	unsigned char *Get_Ver (void)
功能说明	获取CIOS版本号
函数参数	无
返回值	版本号起始地址
相关参考	无
注意事项	无

A.1.3 RF\_Start

函数原型	void RF_Start(unsigned char nFlag)
功能说明	开启/关闭RF射频接口
函数参数	输入： nFlag 1： 开启RF射频接口 0： 关闭RF射频接口 输出： 无
返回值	无
相关参考	无
注意事项	无

A.1.4 RF\_Send

函数原型	unsigned char RF_Send(unsigned char *pData,unsigned short nLen)
功能说明	用于通过RF射频接口发送响应数据
函数参数	输入： pData： 待发送数据区指针； nLen： 待发送数据长度。 输出： 无
返回值	1： 发送成功； 0： 发送失败
相关参考	无
注意事项	无

A.1.5 RF\_Status

函数原型	Unsigned char RF_Status (unsigned char* ucValue, unsigned char Flag)
功能说明	获取RF连接状态
函数参数	输入： Flag =0 为获取链路状态。 Flag =1 保留 输出： Flag =0时， ucValue为输出（0代表断开， 1代表连接） Flag =1时， 保留
返回值	TRUE
相关参考	无
注意事项	无

A.1.6 Get\_ICID

函数原型	unsigned char Get_ICID (unsigned char *pBuff, unsigned int nLen)
功能说明	获取卡片唯一标识
函数参数	输入： nLen:需要产生的ICID字节数。 输出： pBuff:存放ICID的指针
返回值	TRUE:获取成功。 False:获取失败
相关参考	无
注意事项	无

A.1.7 SIM\_APDU\_Transmit

函数原型	unsigned short SIM_APDU_Transmit(unsigned char *byAPDU,unsigned short byAPDU Length, unsigned char *byAPDU_Result, unsigned short *byAPDU_Result_Length)
功能说明	实现RF射频接口模块与电信模块之间的数据转发 (本函数仅适用于双模块结构)
函数参数	输入: *byAPDU: 发送的指令数据。 byAPDU_Length: 发送的指令数据总长度。 输出: *byAPDU_Result: SIM应答数据。 *byAPDU_Result_Length: 应答数据总长度
返回值	指令响应值SW1SW2
相关参考	无
注意事项	接收到RF射频接口数据后 (RF_APDUData_Process_Function中) 调用

A.2 HOOK接口

A.2.1 COSFun\_Param\_Init

函数原型	void COSFun_Param_Init(void)
功能说明	Hook函数, 用于COS层全局变量、文件系统初始化
函数参数	无
返回值	无
相关参考	无
注意事项	无

A.2.2 RF\_APDUData\_Process\_Function

函数原型	unsigned char RF_APDUData_Process_Function(unsigned char *Receivebuff ,unsigned short Receivelen, unsigned char SourceTag)
功能说明	Hook函数, 用于将RF射频接口接收到的数据上传给COS进行处理, 并获取处理结果, 然后通过RF射频接口进行发送
函数参数	输入: Receivebuff: APDU数据起始地址。 Receivelen: 接收数据长度。 SourceTag:: 0: 数据来源为近距离支付交易。 其他: 保留
返回值	1: 发送成功; 其他: 发送失败
相关参考	无
注意事项	无



A.2.3 Check\_OutgoingData\_Hook

函数原型	unsigned char Check_OutgoingData_Hook(unsigned short ucLe, unsigned char *byApduHead, unsigned char *byApduBody, unsigned char *bySW)
功能说明	Hook接口, 监控电信模块指令返回的执行结果, 并由COS决定是否对执行结果进行处理。 (本函数仅适用于双模块结构)
函数参数	输入: ucLe: 非0表示有Le数据。 ByApduHead: APDU命令头。 byApduBody: APDU命令体(Lc)。 bySW: SW值。 输出: byApduBody: APDU返回数据(Le)。 bySW: SW值
返回值	返回数据的长度
相关参考	无
注意事项	Lc情况可修改bySW Le情况可修改byApduBody+bySW

A.2.4 Find\_7816APDU\_Instruction

函数原型	BOOLEAN Find_7816APDU_Instruction(unsigned char *byAPDU, unsigned short *pIndex)
功能说明	Hook函数, CIOS调用, 用于查找COS支持的指令列表, 判断7816接口模块接收到的指令, 是否为COS所需要处理的指令
函数参数	输入: *byAPDU: APDU指令头。 输出: *pIndex: 查到的指令在COS指令列表中的位置索引
返回值	TRUE: COS指令。 FALSE: 非COS指令
相关参考	无
注意事项	COS不需要执行该指令

A.2.5 Get\_7816APDU\_Instruction\_Description

函数原型	unsigned char Get_7816APDU_Instruction_Description(unsigned short unIndex, unsigned char byOffset)
功能说明	Hook函数, 获取指令属性, 并根据指令属性决定是否修改指令数据和/或改变指令传送方向

函数参数	输入： unIndex: 指令在COS指令列表中位置; byOffset: 指令属性的偏移地址。 输出: byResult: 指令的属性值
返回值	TRUE-获取属性值成功; FALSE-获取到了指令属性值,但期望改变指令的传输属性
相关参考	无
注意事项	无

A.2.6 Monitor\_IncomingAPDU\_Instruction

函数原型	BOOLEAN Monitor_IncomingAPDU_Instruction(unsigned char byType, unsigned char *byApduHead,unsigned char *byApduBody)
功能说明	Hook函数, 7816接口命令监控, 对于Lc类型的指令, 由COS决定是否进行指令数据的修改、或改变指令的传输方向
函数参数	输入: byType: APDU类型, 0为Le, 1为Lc。 byApduHead: APDU指令头。 byApduBody: Lc类型的APDU命令体。 输出: byApduBody: Lc类型的APDU命令体
返回值	TRUE-执行监控操作后, 需要进行指令的执行; FALSE-执行了监控操作, 并改变了指令的传输方向
相关参考	无
注意事项	无

A.2.7 Exec\_COS\_Instruction

函数原型	unsigned char Exec_COS_Instruction(unsigned short unIndex, unsigned char *byApduHead,unsigned char *byApduBody,unsigned short *unLeLength,unsigned short*unSW1SW2)
功能说明	Hook函数, 执行7816接口命令并返回执行结果
函数参数	输入: unIndex: 指令在COS指令列表中位置; byApduHead: APDU指令头。 byApduBody: Lc类型的APDU命令体。 输出: byApduBody: Lc类型的APDU命令体。 unLeLength: 返回数据长度。 unSW1SW2: 返回的SW值

返回值	0x80: 将byApduBody中的执行结果返回给移动终端。 0x01: 将byApduBody中的执行结果作为下一条APDU指令的数据体
相关参考	无
注意事项	无

A.2.8 Cos\_process\_instruction\_not\_in\_table

函数原型	void Cos_process_instruction_not_in_table(unsigned char *byApduHead,unsigned short *bySW)
功能说明	HOOK 接口，对于COS不识别的指令，返回处理结果。 （本函数仅适用于单模块结构）
函数参数	输入： byApduHead: APDU指令头。 输出： bySW: 返回的SW值
返回值	无
相关参考	无
注意事项	无

附录 B  
(规范性附录)  
CIOS TPDU 接口

B.1 系统接口

B.1.1 ISO7816VMIInit

函数原型	unsigned char ISO7816VMIInit(void)
功能描述	初始化 7816 接口数据接收环境
函数参数	无
返回值	TRUE--初始化完成
相关参考	无
注意事项	每处理完一条指令（从 7816 接口看来）均需调用该函数才能开始下一条指令的接收，（请参考附录 D.2 CIOS TPDU 接口使用范例）

B.1.2 7816S\_RecvByte

函数原型	unsigned char 7816S_RecvByte(void)
功能描述	从与移动终端相连接的 7816 接口上接收一个字节的数据
函数参数	无
返回值	接收到的一字节数据
相关参考	无
注意事项	必须符合 7816 的 T=0 传输协议

B.1.3 7816S\_SendByte

函数原型	void 7816S_SendByte(unsigned char ByteToSend)
功能描述	从与移动终端相连接的 7816 接口上发送一个字节数据
函数参数	待发送的一字节数据
返回值	无
相关参考	无
注意事项	必须符合 7816 的 T=0 传输协议



B.1.4 GetSIMResponse

函数原型	void GetSIMResponse(unsigned short* BodyLen, unsigned char *byApduHead, unsigned char * byApduBody, unsigned char *bySW, unsigned char transferTag)
功能描述	COS 调用该接口获取电信模块的应答数据，即该函数向电信模块发送指令数据，并接收电信模块指令执行的响应数据 (本函数仅适用于双模块结构)
函数参数	输入参数: BodyLen: 指向数据体长度的指针，当数据体是 Lc 数据时，该指针指向的内容需赋值作为入口参数；当数据体是 Le 数据时，该指针指向的内容会被赋值为 Le 数据长度作为出口参数。 byApduHead: APDU 命令头首址。 byApduBody: APDU 数据体首址。 transferTag: 传输方向标识。 0: COS 层不控制单条指令传输方向，仅监控传输结果（用于 COS 不清楚 SIM 传输方向时交由 CIOS->SIM 传输处理）。 1: COS 层控制传输方向，传输命令和应答数据（用于 COS 主动发送和获取 APDU 层执行结果）。 输出参数: bySW: 指向 SW 值的指针 BodyLen: Le 数据长度；当 BodyLen 返回非 0 且 transferTag=0 时，需在 WT 时间内发送 Le 数据体和 SW（WT 定义参照 7816-3 协议）。 byApduBody: 返回的 Le 数据
返回值	无
相关参考	无
注意事项	必须符合 7816 的 T=0 传输协议

B.1.5 CosBridge

函数原型	void CosBridge(unsigned char* byAPDUHeader)
功能描述	将 TPDU 接口数据转发至 APDU 接口进行处理
函数参数	byAPDUHeader,, APDU 命令头首址
返回值	无
相关参考	无
注意事项	必须符合 7816 的 T=0 传输协议

B.2 Hook接口

B.2.1 ISO7816\_VM

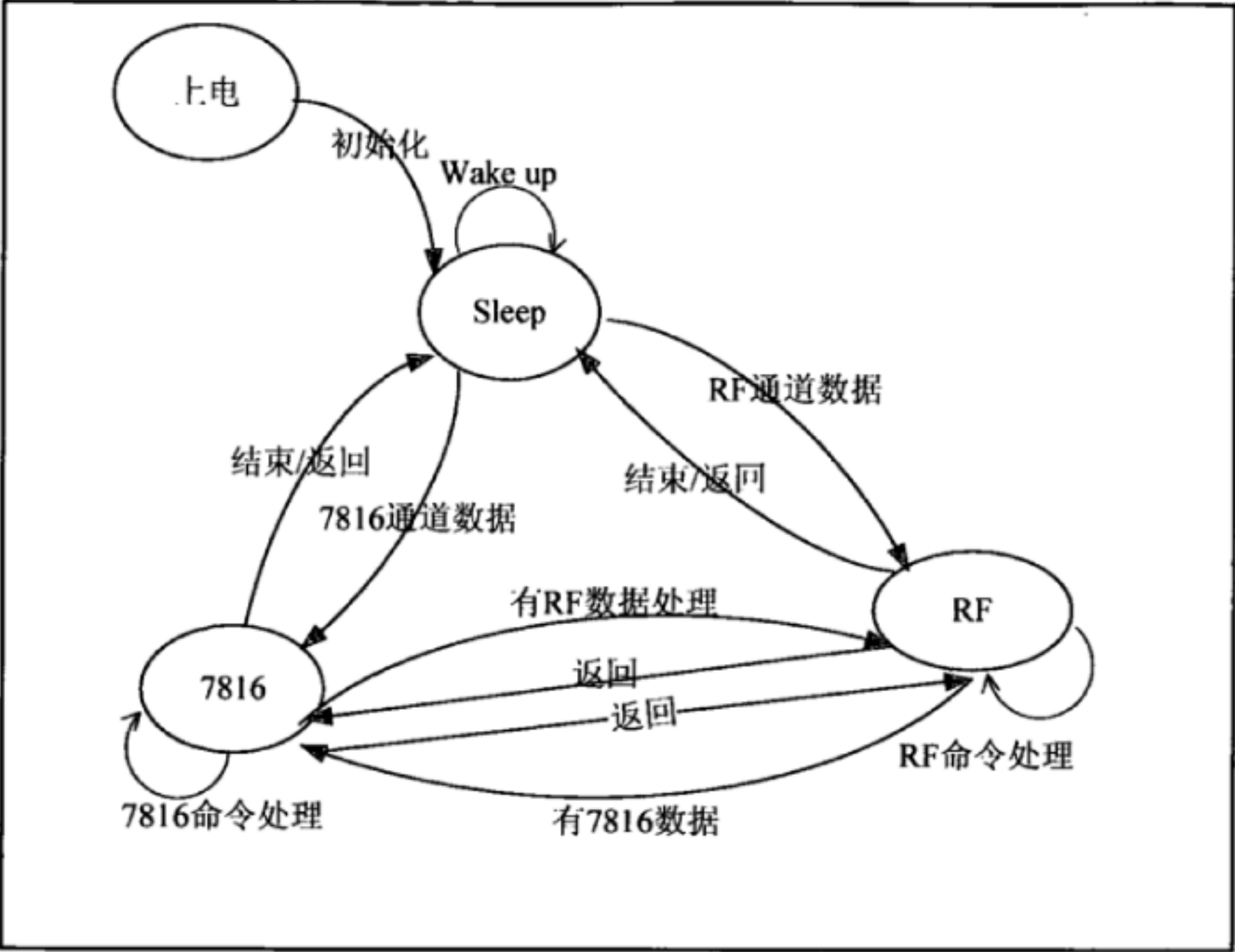
函数原型	void ISO7816_VM(void)
功能描述	COS 层 7816 接口指令处理入口
函数参数	无
返回值	无
相关参考	无
注意事项	无

附录 C  
(资料性附录)  
CIOS/COS 技术特性

C.1 运行机制

C.1.1 工作状态描述

状态控制和转换由CIOS控制，RF-(U)SIM卡工作状态如图C.1所示。



图C.1 RF-(U)SIM卡工作状态

C.1.2 上电状态

系统上电时完成初始化工作，包括在HOOK接口COSFun\_Param\_Init中完成COS变量及函数初始化等。

C.1.3 休眠状态

CIOS管理RF-(U)SIM的休眠和省电模式，当7816和RF接口不在工作状态时自动进入休眠。

C.1.4 RF处理状态

当系统检测到有RF射频通道数据时，进入RF处理状态。CIOS接收到RF数据后，调用COS HOOK接口RF\_APDUData\_Process\_Function进行数据处理。COS在完成RF\_APDUData\_Process\_Function指令处理后，调用RF\_SEND接口发送RF指令执行结果。

C.1.5 7816处理状态

当系统检测到有7816通道数据时，进入7816处理状态。CIOS通过Find\_7816APDU\_Instruction获取COS可执行的指令列表，并通过Exec\_COS\_Instruction执行该指令。



## 附录 D

## (资料性附录)

## COS 开发及接口使用范例

## D.1 基于CIOSAPDU接口开发范例

## D.1.1 7816应用开发

## D.1.1.1 指令散转表

首先, 用户需要建立指令散转表, 声明COS要处理的指令。CIOS通过调用Find\_7816APDU\_Instruction函数得知COS层需要处理该指令, 随后会将指令的处理权交给COS, 否则就会透传到SIM卡中。

散转表设置的结构类型如下:

```
typedef struct
{
    uint8  byINS;
    uint8  byCLA;
    uint8  byINS_Attribute_1;
    uint8  byINS_Attribute_2;
    uint16 (*INS_Address)(uint8 *pAPDU, uint16 *byLeLength, uint8 *byAPDU_Result);
} 7816SAPDU_Attribute;
```

其中, byINS\_Attribute\_1的最高bit位用于标识该指令是否具有Lc类型的数据, 是则为1, 否则为0。byINS\_Attribute\_2用于标识该指令的数据流向, 如果为Only\_HoldUp\_INS, 则COS层将会首先获得该指令的处理权, COS可以决定该指令自己执行还是再传给SIM卡; 如果为Only\_Transfor\_INS, 则表示该指令由COS层发向SIM卡。\*INS\_Address为该指令的处理函数接口。

## D.1.1.2 指令处理权获取 (Find\_7816APDU\_Instruction)

Find\_7816APDU\_Instruction函数会查找COS指令散转表, 如果在散转表中表明COS要处理该指令, CIOS完成APDU指令数据接收后就将完整的APDU数据交给COS层。

例如, COS层私有功能指令, 其byINS\_Attribute\_2字段均为Only\_HoldUp\_INS类型, 再根据指令类型设置byINS\_Attribute\_1, Lc类型的为0×80, 没有Lc类型的为0×00。CIOS会将这些指令都发送给COS处理。

当COS层需要更改某条指令的内容后再将指令传给SIM卡时, 应将byINS\_Attribute\_2字段先设置为Only\_HoldUp\_INS类型, 再后后续函数Monitor\_IncomingAPDU\_Instruction更改指令传输方向。

当COS层仅需要监控某条GSM11.11指令处理的状态, 可以直接调用Check\_OutgoingData\_Hook函数, 这时, 不需要将指令加入散转表。

## D.1.1.3 指令属性获取 (Get\_7816APDU\_Instruction\_Description)

Get\_7816APDU\_Instruction\_Description函数用于获取散转表中指令的属性, 包括指令的传输方向和指令的数据类型。指令的传输方向的设置主要是用于COS层能够监控发送给SIM卡的指令, 便于增加扩展应用。指令数据类型则用于CIOS层通道传输, CIOS层接到5字节指令头后获取指令数据类型, 当指令类型为Lc的情况时, CIOS向设备端返回INS字节以便获取后续数据, 等全部数据接收完成后将完整的APDU指令发送给COS层处理; 当指令类型为Le的情况时, CIOS直接将指令数据发送给COS层处理, COS

层处理完成后将数据和SW值返回给CIOS即可。由此看出，7816指令处理过程中，COS层不需要处理协议层，包括回应INS、发送数据、发送等待字节和SW值，从而大大简化了COS层的处理流程。

#### D.1.1.4 输入指令数据监控 (Monitor\_IncomingAPDU\_Instruction)

COS通过Monitor\_IncomingAPDU\_Instruction函数修改指令传输方向或者指令内容，也可以通过监控指令来触发其他的扩展应用。

输入指令按照数据为Lc类型和Le类型分别进行处理。当改变了指令传输方向，函数返回为FALSE，否则为TRUE。

例如，要想将SIM卡的时钟停止方案改为时钟不停止，需要监控SELECT MF/DF指令。做法是先将select指令添加到指令散转表，属性为“Have\_Lc”和“Only\_HoldUp\_INS”，在Monitor\_IncomingAPDU\_Instruction函数LC类型处理分支中增加如下处理：

```
Flag_MForDF = 0;
if( ((byAPDU[6]==0x3F)&&(byAPDU[7]==0x00))||
    ((byAPDU[6]==0x7F)&&(byAPDU[7]==0x10))||
    ((byAPDU[6]==0x7F)&&(byAPDU[7]==0x20))||
    ((byAPDU[6]==0x7F)&&(byAPDU[7]==0x21)))
{
    Flag_MForDF = 1;
}
bRt = FALSE;
```

其中，Flag\_MForDF标志用于标识指令是否为选择MF/DF的指令，“1”为是，“0”为不是。然后将函数返回值设置为FALSE。

在后续函数Check\_OutgoingData\_Hook函数中增加以下处理：

```
if((byApduHead[1]==0xF2)
    ||((byApduHead[1]==0xC0)&&(Flag_MForDF==1)))
{
    if (ucLe!=0) //有LE数据
    {
        byApduBody[13] = (byApduBody[13]&0xF2);
    }
}
```

通过在两个Hook函数中增加相关处理，最终将选择MF/DF的get response指令和STATUS指令返回值中的支持时钟字节更改为时钟不停止。

#### D.1.1.5 指令分发处理 (Exec\_COS\_Instruction)

Exec\_COS\_Instruction函数根据指令散转表跳转到相应指令处理模块，输入参数为指令APDU完整数据，函数输出包括指令的处理结果以及是否需要向SIM卡再发送指令。

用户可以在指令跳转前再增加数据处理，也可以根据需求不进入指令处理模块而进行其他操作。

例如，生成随机数指令时设置：rnd\_num=1;



在Exec\_COS\_Instruction增加以下处理:

```
if (g_byBakINS != 0x84)
{
    rnd_num = 0;
}
g_byBakINS = byAPDU[1];
```

函数功能是当上一条指令不是生成随机数指令时置随机数无效, 保证当前指令在没有取随机数时无法执行。

COS收到一条指令处理后希望再触发向SIM卡发送另外一条指令的处理流程可以通过函数返回Need\_Multi\_APDU值实现。用户可以通过该功能处理应用层指令或者扩展应用。例如, COS层处理应用时需要从SIM卡上获取数据, 就可以通过CIOS发送指令给SIM卡得到。

#### D.1.1.6 输出数据监控 (Check\_OutgoingData\_Hook)

利用Check\_OutgoingData\_Hook函数可以对SIM卡指令输出数据进行监控和修改。在上述示例中通过和Monitor\_IncomingAPDU\_Instruction函数配合, 修改了SIM卡get response和status指令的输出。这个函数可以满足扩展应用的需求。

在这个函数中, 用户也可以根据SIM卡的返回值再次发起一条指令发送给SIM卡, 机制和Exec\_COS\_Instruction函数中描述的相同, 只是接口位置不同。在这里用户可以利用SIM卡的返回值作为触发条件。

#### D.1.2 RF应用开发

CIOS为RF应用开发提供了一个Hook函数RF\_APDUData\_Process\_Function和一个API函数SIM\_APDU\_Transmit。CIOS通过RF\_APDUData\_Process\_Function函数将SCR通道接收的RF数据传递给COS, COS在RF\_APDUData\_Process\_Function函数中增加应用处理, 并将需要返回的数据回传给CIOS, CIOS将数据发送到SCR通道。通过这样的机制, COS层不再需要调用SCR发送接收函数, 只需进行数据的应用处理就可以了。CIOS提供的API函数SIM\_APDU\_Transmit用于COS层向SIM通道发送数据, 这时COS层相当于设备端的应用, SIM\_APDU\_Transmit函数负责数据的发送和接收。

##### D.1.2.1 RF hook函数 (RF\_APDUData\_Process\_Function)

RF\_APDUData\_Process\_Function函数作为COS层处理RF应用的接口, 首先根据数据或应用判断指令的传输方向, 如果是COS层处理则转入函数处理模块, 如果要发送给SIM卡则调用SIM\_APDU\_Transmit函数。COS层整理最终的处理结果返回给CIOS层。

COS判断指令传输方向也是利用指令散转表, 由COS处理的指令都加入RF指令散转表中。用户可以根据应用制定个性的模式。

```
if(Find_RFAPDU_Instruction(Receivebuff,&unCommand_Index))
{
    unSW1SW2=
    (COS_APDU_FIX_INS[unCommand_Index].INS_Address)(Receivebuff,&unRececvLen,byTemprecv
    Buff);
```

```

    }
    else
    {
        //向SIM透传指令，可以在传递前修改指令内容或增加其他处理
        unSW1SW2 = SIM_APDU_Transmit(Receivebuff,&Receivelen,byTemprecvBuff,&unRececvLen);
        byDataType = 1;
    }
    ret = RF_Send(byTemprecvBuff, unRececvLen);
    return ret;

```

#### D.1.2.2 RF API函数

SIM\_APDU\_Transmit函数功能类似于PC/SC协议的驱动函数，用于7816协议通道的数据传输。用户调用该函数后就不需要关心通道的传输协议了。

处理完成后调用RF\_Send接口发送结果并将返回值传递给RF\_APDUData\_Process\_Function。

### D.2 CIOS TPDU接口使用范例

#### D.2.1 7816 TPDU接口应用开发

ISO7816\_VM流程框架如下：

```

void ISO7816_VM(void)
{
    uint8 ret;
    while(1)
    {
        ret=ISO7816VMInit();
        if(ret==0x01)
        {
            uint8 7816S_Apdu[5];
            uint8 7816Buf[256];
            uint8 SWBuf[2];
            uint8 i;
            for(i=0; i<5; i++)
            {
                7816S_Apdu[i]=7816S_RecvByte(); //接收APDU指令头
            }
            if(7816S_Apdu[0] != 0xa0)
            {
                COSCmdProc(7816S_Apdu); //模式4 COS 私有指令
            }
            elseif(7816S_Apdu[1] == 0xc2) //模式2 COS监控指令

```

```
{
    Get_SIM_Response (lc, 7816S_Apdu, 7816Buf, SWBuf,0)
    if (SWBuf[0] ==0x95 && SWBuf[1]==0x00)
    {
        //整理新的APDU指令数据
        Get_SIM_Response (lc,7816S_Apdu,7816Buf,SWBuf, 0) //模式5 SIM私有指令
    }
    7816S_SendByte(SWBuf[0]);
    7816S_SendByte(SWBuf[1]);
}
else
{
    Cos_Bridge(7816S_Apdu); //模式1 透传指令
}
}
}
}
```

---



中 华 人 民 共 和 国  
通 信 行 业 标 准

手机支付

基于 2.45GHz RCC(限域通信)技术的智能卡技术要求

YD/T 2774-2014

\*

人民邮电出版社出版发行

北京市丰台区成寿寺路 11 号邮电出版大厦

邮政编码: 100164

北京康利胶印厂印刷

版权所有 不得翻印

\*

开本: 880 × 1230 1/16

2015 年 12 月第 1 版

印张: 2

2015 年 12 月北京第 1 次印刷

字数: 32 千字

15115 · 605

定价: 20 元

本书如有印装质量问题, 请与本社联系 电话: (010)81055492