



矽鼎 Kivvi 支付终端

第三方应用设备接口规范

第 2.1.9 版

无锡矽鼎科技有限公司
二〇一七年六月二十日

版本控制信息

版本	日期	拟稿和修改	说明
2.0.0	2016.06.22	吴娟 (Joyce)	初稿
2.0.1	2016.07.07	陈俊俊 (George)	完善接口定义和指令说明
2.0.2	2016.07.11	郁丽 (Lucy)	完善接口定义和指令说明
2.0.3	2016.07.28	陈俊俊 (George)	“搜卡”、“交易请求”和“EMV 交易”指令增加磁道数据加密说明。
2.0.4	2016.10.28	陈俊俊 (George)	完善密钥管理体系的说明
2.0.5	2016.11.11	陈俊俊 (George)	增加 isbusy 指令和 led 控制指令； 密码输入时增加无密码直接确认的配置参数 noPinFormat； 完善 apdu 指令功能，支持 IC 卡
2.0.6	2016.12.17	杨东林(Neil)	增加 pinprocess 指令中 pinFormat 参数的“PLAIN_TEXT”明文密码有效值 增加 qrcode 指令中可选参数 payType，用于在二维码中间显示支付类型 LOGO
2.0.7	2017.01.03	陈俊俊 (George)	增加 DUKPT 的 KSN 操作指令
2.1.0	2017.03.09	朱广伟 (Scott)	银行卡，EMV 交易指令参数部分重新定义，增加对电子现金功能的支持，包括电子现金余额查询和交易记录查询功能。
2.1.1	2017.03.13	朱勇敏(Eddard)	增加串口指令
2.1.2	2017.03.23	杨东林(Neil)	增加秘钥加载使用流程图
2.1.3	2017.03.24	朱广伟(Scott)	交易请求指令，增加“transFlow”字段
2.1.4	2017.03.27	杨东林(Neil)	增加“密钥分配及管理规则”
2.1.5	2017.04.01	朱广伟(Scott)	加载 EMV 参数部分，增加终端参数配置的功能
2.1.6	2017.04.05	金晖(Martin)	添加小屏数字签名功能。 小屏 LOGO 及轮播图片支持 256 色位 bmp 图片。添加 emv 参数配置指令。
2.1.7	2017.04.06	朱广伟(Scott)	下载 EMV 参数添加对多应用的支持，增加 appId 字段
2.1.8	2017.04.17	朱勇敏(Eddard)	添加等待打印机打印结束指令
2.1.9	2017.06.19	金晖(Martin)	更新指令参数配置说明 添加 appId 分配说明

目录

1. 概述	5
2. 类与接口定义	5
2.1. 结果监听接口类 KivviDeviceRespListener	5
2.2. 设备类 KivviDevice	5
3. 操作定义	6
3.1. 指令类型	6
3.2. 指令列表	7
3.3. 指令及参数详细说明	8
3.3.1. 基本操作	8
3.3.1.1. 读取版本号	8
3.3.1.2. 时间操作	9
3.3.1.3. 系统操作	9
3.3.1.4. 读取 BUSY 态	9
3.3.1.5. LED 控制	10
3.3.2. 银行卡	10
3.3.2.1. 搜卡	10
3.3.2.2. EMV 交易	11
3.3.2.3. 交易请求	12
3.3.2.4. 发卡行数据处理	14
3.3.2.5. 检测 IC 卡槽	15
3.3.2.6. Mifare 卡操作	15
3.3.2.7. APDU 操作	16
3.3.2.8. 芯片卡脱机读取卡片余额	16
3.3.2.9. 芯片卡读取交易记录	16
3.3.2.10. 配置 EMV 参数	16
3.3.3. PINPAD 操作	17
3.3.3.1. 加载密钥	17
3.3.3.2. 输密码	19
3.3.3.3. 加解密	19
3.3.3.4. 计算 MAC	20
3.3.3.5. 随机数生成	20
3.3.3.6. 读取/更新 KSN	20
3.3.3.7. 敏感信息确认	21
3.3.3.8. 数字签名	21
3.3.4. 文件存储	21
3.3.4.1. 保存文件	21
3.3.4.2. 读取文件	22
3.3.4.3. 删除文件	22
3.3.4.4. 保存图片 (Bitmap)	22
3.3.4.5. 加载 EMV 参数	23
3.3.5. 屏幕显示	23
3.3.5.1. 显示待机 Logo	23
3.3.5.2. 显示轮播图片	23
3.3.5.3. 显示客户信息	24
3.3.5.4. 显示二维码	24

- 3.3.6. 打印操作 24
 - 3.3.6.1. 缺纸检查 24
 - 3.3.6.2. 打印文字 24
 - 3.3.6.3. 走纸 25
 - 3.3.6.4. 打印一维码 25
 - 3.3.6.5. 打印二维码 25
 - 3.3.6.6. 打印图片 26
 - 3.3.6.7. 等待打印结束 26
 - 3.3.7. 串口操作 26
 - 3.3.7.1. 打开串口 26
 - 3.3.7.2. 关闭串口 26
 - 3.3.7.3. 接受数据 27
 - 3.3.7.4. 发送数据 27
 - 4. 错误码定义 27
 - 5. 密钥分配及管理规则 28
 - 5.1 密钥总数 28
 - 5.2 密钥分配原则 28
 - 5.2.1 密钥的相互独立性 28
 - 5.2.2 单个 App 密钥组数..... 28
 - 5.2.3 密钥的起始位置 28

1. 概述

这套接口为矽鼎智能终端（Par6 和 Par10）外设统一接口，以便于上层应用开发。

2. 类与接口定义

2.1. 结果监听接口类 KivviDeviceRespListener

```
public interface KivviDeviceRespListener {
    void onResponse(KivviDeviceResp kivviDeviceResp);
}
```

结果类: KivviDeviceResp
暂时只有一个成员: int ErrCode (*)
*关于错误码定义，请参考：第四节错误码定义。

2.2. 设备类 KivviDevice

原型定义	int Set(String key, Object value)	
功能	设备行为参数设置	
参数	key	参数名 *
	value	参数值。只支持 String、int、byte[]三种类型，其他包括 null 在内都不支持
返回	错误码	

* 关于参数名，请参考：第二节参数定义与实例

原型定义	int Action(String cmd [, final KivviDeviceRespListener listener])	
功能	执行具体的设备行为	
参数	cmd	行为指令
	listener	异步行为指令结果监听器
返回	错误码	

原型定义	Object Get(String key [, int exParam])	
功能	读取结果	
参数	key	结果数据名
	exParam	结果数据附加参数（可选）
返回	结果数据 Object 对象，如不存在返回 null	

原型定义	String GetString(String key [, int exParam])	
功能	读取 String 类型结果。（扩展于 Get 方法）	

参数	key	结果数据名
	exParam	结果数据附加参数（可选）
返回	结果数据 String 对象，如不存在返回 null	

原型定义	<code>byte[] GetByteArray(String key [, int exParam])</code>	
功能	读取 byte[] 类型结果。（扩展于 Get 方法）	
参数	key	结果数据名
	exParam	结果数据附加参数（可选）
返回	结果数据 byte[] 对象，如不存在返回 null	

原型定义	<code>intGetInt(String key [, int exParam])</code>	
功能	读取 int 类型结果（扩展于 Get 方法）	
参数	key	结果数据名
	exParam	结果数据附加参数（可选）
返回	结果数据 int 值，如不存则抛出异常	

原型定义	<code>boolean GetBool(String key [, int exParam])</code>	
功能	读取 boolean 类型结果（扩展于 GetInt 方法）	
参数	key	结果数据名
	exParam	结果数据附加参数（可选）
返回	结果数据 boolean 值，如不存则抛出异常	

原型定义	<code>boolean Has(String key [, int exParam])</code>	
功能	判断 key 是否存在	
参数	key	结果数据名
	exParam	结果数据附加参数（可选）
返回	存在返回 true，不存在则返回 false	

3. 操作定义

3.1. 指令类型

指令类型	指令定义	所需权限	功能说明
卡操作	"card."	KIVVI_CARD	银行卡和交易类操作

PINPAD 操作	"pinpad."	KIVVI_PINPAD	密码键盘相关操作，如密码输入、数据加解密、MAC 计算等
文件存储	"storage."	KIVVI_STORAGE	文件存储操作、存储 EMV 参数、清除 EMV 参数等
屏幕显示	"exscreen."	KIVVI_EXSCREEN	显示二维码、显示用户信息
基本操作	"basic."	至少包含以上一种权限	获取时间、设置时间、获取版本等
打印操作	"printer."	KIVVI_PRINTER	打印机检测操作、打印操作

*注：在使用上述指令类型时，必须在 **AndroidManifest** 中配置如下代码：

```
<uses-permission android:name="android.permission.*" />
```

例：配置屏幕显示权限。

```
<uses-permission android:name="android.permission.KIVVI_EXSCREEN" />
```

3.2. 指令列表

类别	指令名称	指令	建议方式	功能说明
基本操作	读取版本号	"basic.cmd.version"	顺序执行	读取金融模块和 SDK 版本信息
	时间操作	"basic.cmd.time"	顺序执行	读取或设置时间
	系统操作	"basic.cmd.system"	顺序执行	系统级操作，如重启模块
	读取 BUSY 态	"basic.cmd.isbusy"	顺序执行	固件是否处于 BUSY 状态
	LED 控制	"basic.cmd.led"	顺序执行	控制固件的 LED 灯
银行卡	搜卡	"card.cmd.search"	异步执行	提示并等待用户搜卡
	EMV 交易	"card.cmd.emv_process"	异步执行	EMV 交易请求
	交易请求	"card.cmd.transact"	异步执行	银行卡交易请求，提示用户刷(插/挥)卡和输密码
	发卡行数据处理	"card.cmd.issuer_process"	顺序执行	EMV 交易的发卡行数据处理
	检测 IC 卡槽	"card.cmd.detect_ic_slot"	顺序执行	检测 IC 卡槽是否有卡
	Mifare 卡操作	"card.cmd.mifare"	顺序执行	Mifare 卡的认证、读写等
	APDU 操作	"card.cmd.apdu"	顺序执行	APDU 交互操作
	电子现金脱机余额查询	"emv.cmd.balance"	顺序执行	电子现金脱机余额查询（注：先要执行搜卡“card.cmd.search”指令）
	芯片卡交易记录查询	"emv.cmd.log"	顺序执行	芯片卡交易记录查询（注：先要执行搜卡“card.cmd.search”指令）
	配置 EMV 参数	"emv.cmd.paramset"	顺序执行	国家/货币代码参数配置。
PINPAD	加载密钥	"pinpad.cmd.loadkey"	顺序执行	加载 KPK、主密钥、工作密钥
	输密码	"pinpad.cmd.pinprocess"	异步执行	提示并等待用户输入密码

	加解密	"pinpad.cmd.crypto"	顺序执行	测试加解密功能
	计算 MAC	"pinpad.cmd.mac"	顺序执行	计算 MAC
	随机数生成	"pinpad.cmd.random"	顺序执行	生成随机数
	敏感信息确认	"pinpad.cmd.confirm"	异步执行	余额等敏感信息确认
	读取/更新 KSN	"pinpad.cmd.ksn"	顺序执行	读取/更新 KSN
	数字签名	"pinpad.mpr.handwrite"	顺序执行	小屏手写签名。
文件存储	保存文件	"storage.mpw.write_file"	顺序执行	存储文件
	读取文件	"storage.mpr.read_file"	顺序执行	读取文件
	删除文件	"storage.cmd.delete_file"	顺序执行	删除文件
	加载 EMV 参数	"storage.cmd.load_emvparams"	顺序执行	加载 EMV 参数
	保存图片	"storage.mpw.load_bitmap"	顺序执行	保存位图或 logo (支持 256 色 bmp 位图)
屏幕显示	待机	"exscreen.cmd.idle"	顺序执行	小屏显示待机 Logo
	显示二维码	"exscreen.cmd.qrcode"	顺序执行	小屏显示二维码
	图片轮播	"exscreen.cmd.bitmap"	顺序执行	小屏图片轮播
	显示用户信息	"exscreen.cmd.custom_msg"	顺序执行	小屏显示用户自定义信息
打印操作	缺纸检测	"printer.cmd.paperout"	顺序执行	打印机缺纸检测
	走纸	"printer.cmd.feed"	顺序执行	打印机走纸
	打印文字	"printer.cmd.text"	顺序执行	打印文字
	打印图片	"printer.cmd.photo"	顺序执行	打印图片
	打印二维码	"printer.cmd.qrcode"	顺序执行	打印二维码
	打印一维码	"printer.cmd.obcode"	顺序执行	打印一维码

3.3. 指令及参数详细说明

参数名:当前指令可以设置或者获取的参数名字

类型: STR String 类型; INT int 类型; BIN byte[]类型

长度: 值的字节数, VAR 表示变长数据

默认值: 对于有定义默认值的参数, 当没有 Set 该参数时, 金融模块直接使用默认值

请求: 输入型参数, 即在 Action 执行前, 可 Set 的参数

响应: 输出型参数, 即在 Action 执行后, 可通过 Get 取得的参数

* 对于指令和参数值, 在 Demo 的 utils/KV.java 有做常量定义, 在开发过程中, 可直接使用文档所写的字符串, 也可使用 KV.java 的定义, 建议后者。

3.3.1. 基本操作

3.3.1.1. 读取版本号

指令: "basic.cmd.version"

参数列表:

参数名	类型	长度	有效取值/默认值	描述
请求				
无				
响应				
"ret"	INT	4		错误码
"result"	STR	VAR		错误描述
"hwVer"	STR	VAR		金融模块硬件版本号
"fwVer"	STR	VAR		软件版本号
"serialNo"	STR	VAR		金融模块序列号
"KivviDeviceSN"	STR	VAR		主设备序列号
"KivviDeviceHardwareVersion"	STR	VAR		主设备硬件版本号
"SdkVerison"	STR	VAR		SDK 版本
"KivviDeviceVerison"	STR	VAR		KivviDevice 版本
"KivviDevicePlatform"	STR	VAR		KivviDevice 平台

代码参考: action/basic/ActionGetVersion.java

3.3.1.2. 时间操作

指令: "basic.cmd.time"

参数列表:

参数名	类型	长度	有效取值/默认值	描述
请求				
"operate"	STR	VAR	"GET" (默认)	读取时间
			"SET"	设置时间
"datetime"	STR	19	"yyyy/mm/dd/hh/mm/ss"	仅"SET"时需要
响应				
"ret"	INT	4		错误码
"result"	STR	VAR		错误描述
"datetime"	STR	19	"yyyy/mm/dd/hh/mm/ss"	

代码参考: action/basic/ActionGetTime.java 和 ActionSetTime.java

3.3.1.3. 系统操作

指令: "basic.cmd.system"

参数列表:

参数名	类型	长度	有效取值/默认值	描述
请求				
"operate"	STR	VAR	"reboot"	重启金融模块
响应				
"ret"	INT	4		错误码
"result"	STR	VAR		错误描述

代码参考: action/basic/ActionRebootPos.java

3.3.1.4. 读取 BUSY 态

指令: "basic.cmd.isbusy"

参数列表:

参数名	类型	长度	有效取值/默认值	描述
请求				
无				
响应				
"ret"	INT	4		错误码
"result"	STR	VAR		错误描述
"isbusy"	INT	4		0 空闲状态; 1 Busy 状态

3.3.1.5. LED 控制

指令: "basic.cmd.led"

参数列表:

参数名	类型	长度	有效取值/默认值	描述
请求				
"led"	STR	VAR	"RED"、"GREEN"、"YELLOW"、"BLUE"、"DRED"、"DGREEN" 自由组合, 用' '分隔	
"operate"	STR	VAR	"ON"、"OFF"、"BLINK"	亮/灭/闪烁
"delay"	INT	4	闪烁亮的时间, 仅 BLINK 时有效。	单位 ms
"speed"	INT	4	闪烁间隔时间, 仅 BLINK 时有效。	单位 ms
响应				
"ret"	INT	4		错误码
"result"	STR	VAR		错误描述

3.3.2. 银行卡

3.3.2.1. 搜卡

指令: "card.cmd.search"

参数列表:

参数名	类型	长度	有效取值/默认值	描述
请求				
"cardType"	STR	VAR	"MSR"、"IC"、"NFC" 自由组合, 用' '分隔, 默认"MSR IC NFC"	
"trackMode"	STR	VAR	"plain" (默认)	磁道明文
			"entype0"	磁道密文, 备注 6.2
			"Unionpay"	磁道密文, 银联加密算法
"keyMng"	STR	VAR	"MKSK" (默认) "DUKPT"一次一密 "FIXED"固定密钥 "JF"即富定制	
"appId"	INT	4	0x01~0x0F 默认 0x01	仅当磁道加密时需要
"timeout"	INT	4	10~120 默认 60	单位秒
"allowFallback"	INT	4	0: 不允许 1: 允许	是否允许降级交易
响应				

"ret"	INT	4		错误码
"result"	STR	VAR		错误描述
"cardType"	STR	VAR	"MSR"、"IC"、"NFC"	
"isICCard"	INT	4	0 非 IC 卡或插反；1 正常 IC 卡	仅当 cardType 为"IC"时存在
"nfcType"	STR	VAR	"typeA"、"typeB"、"M1"	仅当 cardType 为"NFC"时存在
"track1"	STR	VAR		仅当 cardType 为"MSR"时存在
"track2"	STR	VAR		仅当 cardType 为"MSR"时存在
"track3"	STR	VAR		仅当 cardType 为"MSR"时存在
"pan"	STR	VAR		仅当 cardType 为"MSR"时存在
"expDate"	STR	VAR		仅当 cardType 为"MSR"时存在
"withIC"	INT	4	0 无 IC 芯片；1 有	仅当 cardType 为"MSR"时存在

代码参考：action/card/ActionSearch.java

3.3.2.2. EMV 交易

指令：" card.cmd.emv_process"

参数列表：

参数名	类型	长度	有效取值/默认值	描述
请求				
"amount"	STR	VAR		交易金额（可选）
"amountOther"	STR	VAR		其他金额（可选）
"transType"	INT	4	1: 消费 2: 撤销 3: 退货 4: 联机余额查询 5: 预授权 6: 预授权撤销 7: 预授权完成请求 8: 预授权完成通知 9: 预授权完成撤销 11: 电子现金余额查询 12: 电子现金圈存 13: 电子现金消费 14: 电子现金非指定账户圈存 15: 电子现金指定账户圈存	交易类型码
"transFlow"	INT	4	1: 完整流程 2: 简化流程（芯片卡只读取卡号等参数）	芯片卡交易流程，完整流程是执行完整的芯片卡交易流程，联机或脱机；简化流程只读卡芯片卡卡号等必要信息。详细参考《销售点终端 POS 应用规范》中的说明。
"keyMng"	STR	VAR	"MKSK"（默认） "DUKPT"一次一密 "FIXED"固定密钥 "JF"即富定制	密钥管理体系
"pinFormat"	STR	VAR	"FORMAT0"（默认）	PINBLOCK 格式

			"FORMAT1", "FORMAT3"	
"trackMode"	STR	VAR	"plain" (默认)	磁道明文
			"entype0"	磁道密文, 备注 6.2
			"Unionpay"	磁道密文, 银联加密算法
"appId"	INT	4	0x01~0x0F 默认 0x01	
"timeout"	INT	4	10~120 默认 60	单位秒
"pinMinLen"	INT	4	4~12 默认 4	密码最短长度
"pinMaxLen"	INT	4	4~12 默认 12	密码最长长度
"isForceOnline"	INT	4	0: 非强制联机 (默认) 1: 强制联机	强制联机标志 (注: 非电子现金交易, 此参数要设置为 1)
"isSupportEC"	INT	4	0: 非电子现金交易 (默认) 1: 电子现金交易	电子现金交易标志
"isSupportCVM"	INT	4	0: 不执行 CVM 1: 执行 CVM (默认)	芯片卡交易 CVM 执行标志
"isUsePinpad"	INT	4	1: 输 PIN 由 EMV 内核控制 (默认)	是否使用 EMV 内核控制的密码键盘
			0: 输 PIN 由应用控制, 应用要调用 "pinpad.cmd.pinprocess" 指令	
"reqTagList"	STR	VAR		EMV 数据 Tag 列表, Tag 之间用' '分割 (可选)
响应				
"ret"	INT	4		错误码
"result"	STR	VAR		错误描述
"pan"	STR	VAR		主帐号
"track2"	STR	VAR		二磁道数据
"seqNo"	STR	2		IC 卡序列号
"expDate"	STR	VAR		有效期
"pinBlock"	BIN	8		
"pinpadResult"	STR	VAR	"OK"计算 pinblock 成功 "FAIL"计算 pinblock 失败 "USER CANCEL"用户取消输 PIN "TIMEOUT"用户输 PIN 超时 "NO PIN"用户没有输 PIN, 直接按"确认"	密码键盘结果
"cvmType"	STR	VAR	"ONLINE_PIN"	联机 PIN
			"SIGN"	签名
"emvDataType"	STR	VAR	"REQUEST"请求	EMV 数据类型
			"CONFIRM"确认	
			"REVERSAL"冲正	
"emvData"	BIN	VAR		EMV 数据 (55 域)

代码参考: action/card/ActionEmvProc.java

3.3.2.3. 交易请求

指令: "card.cmd.transact"

参数列表:

参数名	类型	长度	有效取值/默认值	描述
请求				
"amount"	STR	VAR		交易金额（可选）
"amountOther"	STR	VAR		其他金额（可选）
"transType"	INT	4	1: 消费 2: 撤销 3: 退货 4: 联机余额查询 5: 预授权 6: 预授权撤销 7: 预授权完成请求 8: 预授权完成通知 9: 预授权完成撤销 11: 电子现金余额查询 12: 电子现金圈存 13: 电子现金消费 14: 电子现金非指定账户圈存 15: 电子现金指定账户圈存	交易类型
"transFlow"	INT	4	1: 完整流程 2: 简化流程（芯片卡只读取卡号等参数）	芯片卡交易流程，完整流程是执行完整的芯片卡交易流程，联机或脱机；简化流程只读卡芯片卡卡号等必要信息。详细参考《销售点终端 POS 应用规范》中的说明。
"cardType"	STR	VAR	"MSR"、"IC"、"NFC" 自由组合，用' '分隔，默认"MSR IC NFC"	
"keyMng"	STR	VAR	"MKSK"（默认） "DUKPT"一次一密 "FIXED"固定密钥 "JF"即富定制	密钥管理体系
"pinFormat"	STR	VAR	"FORMAT0"（默认） "FORMAT1", "FORMAT3" "PLAIN_TEXT"	PINBLOCK 格式
"trackMode"	STR	VAR	"plain"（默认）	磁道明文
			"entype0"	磁道密文
			"Unionpay"	磁道密文，银联加密算法
"appId"	INT	4	0x01~0x0F 默认 0x01	
"timeout"	INT	4	10~120 默认 60	单位秒
"msrPinProc"	INT	4	0 不输密 1 输密	搜到磁条卡是否进行输密
"pinMinLen"	INT	4	4~12 默认 4	密码最短长度
"pinMaxLen"	INT	4	4~12 默认 12	密码最长长度
"allowFallback"	INT	4	0 不允许 1 允许	是否允许降级交易
"isForceOnline"	INT	4	0: 非强制联机（默认）	强制联机标志（注：非电子现

			1: 强制联机	金交易，此参数要设置为 1)
"isSupportEC"	INT	4	0: 非电子现金交易（默认） 1: 电子现金交易	电子现金交易标志
"isSupportCVM"	INT	4	0: 不执行 CVM 1: 执行 CVM（默认）	芯片卡交易 CVM 执行标志
"isUsePinpad"	INT	4	1: 输 PIN 由 EMV 内核控制（默认）	是否使用 EMV 内核控制的密码键盘
			0: 输 PIN 由应用控制，应用要调用 "pinpad.cmd.pinprocess" 指令	
"reqTagList"	STR	VAR		EMV 数据 Tag 列表，Tag 之间用' '分割（可选）
响应				
"ret"	INT	4		错误码
"result"	STR	VAR		错误描述
"cardType"	STR	VAR	"MSR"、"IC"、"NFC"	
"pan"	STR	VAR		主帐号
"track1"	STR	VAR		
"track2"	STR	VAR		
"track3"	STR	VAR		
"seqNo"	STR	2		IC 卡序列号
"expDate"	STR	VAR		有效期
"pinBlock"	BIN	8		
"pinpadResult"	STR	VAR	"OK"计算 pinblock 成功 "FAIL"计算 pinblock 失败 "USER CANCEL"用户取消输 PIN "TIMEOUT"用户输 PIN 超时 "NO PIN"用户没有输 PIN，直接按"确认"	密码键盘结果
"cvmType"	STR	VAR	"ONLINE_PIN"	联机 PIN
			"SIGN"	签名
"emvDataType"	STR	VAR	"REQUEST"请求	EMV 数据类型
			"CONFIRM"确认	
			"REVERSAL"冲正	
"emvData"	BIN	VAR		EMV 数据（55 域）

代码参考：action/card/ActionTransact.java

3.3.2.4. 发卡行数据处理

指令："card.cmd.issuer_process"

参数列表：

参数名	类型	长度	有效取值/默认值	描述
请求				
"respCode"	STR	2		收单平台响应码，通信失败时不设置
"issuerData"	BIN	VAR		发卡行数据

"reqTagList"	STR	VAR		EMV 数据 Tag 列表, Tag 之间用' '分割 (可选)
响应				
"ret"	INT	4		错误码
"result"	STR	VAR		错误描述
"emvDataType"	STR	VAR	"REQUEST"请求	EMV 数据类型
			"CONFIRM"确认	
			"REVERSAL"冲正	
"emvData"	BIN	VAR		EMV 数据 (55 域)

代码参考: action/card/ActionEmvIssuerProc.java

3.3.2.5. 检测 IC 卡槽

指令: "card.cmd.detect_ic_slot"

参数列表:

参数名	类型	长度	有效取值/默认值	描述
请求				
"isICCard"	INT	4	0 不做上电检测, 1 做上电检测	用来检测 IC 卡有没有反插
响应				
"ret"	INT	4		错误码
"result"	STR	VAR		错误描述
"cardInSlot"	INT	4	0 无卡, 1 有卡	
"isICCard"	INT	4	0 错误卡, 1 IC 卡	仅当有卡时存在

代码参考: action/card/ActionIcslot.java

3.3.2.6. Mifare 卡操作

指令: "card.cmd.mifare"

参数列表:

参数名	类型	长度	有效取值/默认值	描述
请求				
"operate"	STR	VAR	"AUTH"	认证
			"INCREASE"	增值
			"DECREASE"	减值
			"READ"	读数据
			"WRITE"	写数据
"block"	INT	4		操作扇区
"authKeyType"	STR	4	"KeyA"	仅当"AUTH"操作时需要
			"KeyB"	
"authKey"	BIN	6		仅当"AUTH"操作时需要
"num"	INT	4		仅当"INCREASE"或"DECREASE"操作时需要
"data"	BIN	VAR		仅当"WRITE"操作时需要
响应				
"ret"	INT	4		错误码
"result"	STR	VAR		错误描述

"data"	BIN	VAR		仅当"READ"操作时存在
--------	-----	-----	--	---------------

代码参考: action/card/ActionMifare*.java

3.3.2.7. APDU 操作

指令: "card.cmd.apdu"

参数列表:

参数名	类型	长度	有效取值/默认值	描述
请求				
"cardType"	STR	VAR	"IC"	
			"NFC" (默认)	
"operate"	STR	VAR	"OPEN"	IC 卡上电 / 打开 NFC 场强
			"CLOSE"	IC 卡下电 / 关闭 NFC 场强
			"EXCHANGE" (默认)	APDU 数据交互
"data"	BIN	VAR		发送 APDU 数据
"timeout"	INT	4	10~120 默认 60	单位秒
响应				
"ret"	INT	4		错误码
"result"	STR	VAR		错误描述
"data"	BIN	VAR		响应的 APDU 数据

代码参考: action/card/ActionNfcApdu.java

3.3.2.8. 芯片卡脱机读取卡片余额

指令: "emv.cmd.balance"

参数列表:

参数名	类型	长度	有效取值/默认值	描述
请求				
无				
响应				
"ret"	INT	4		错误码
"data"	ASCII	12		脱机卡片余额

代码参考: action/card/ActionEmvBalance.java

3.3.2.9. 芯片卡读取交易记录

指令: "emv.cmd.log"

参数列表:

参数名	类型	长度	有效取值/默认值	描述
请求				
无				
响应				
"ret"	INT	4		错误码
"data"	BIN	VAR		芯片卡交易记录
"logCount"	INT	4		芯片卡交易记录条数 (大于等于 0, 小于等于 10)

代码参考: action/card/ActionEmvLog.java

3.3.2.10. 配置 EMV 参数

指令: "emv.cmd.paramset"

参数列表:

参数名	类型	长度	有效取值/默认值	描述
请求				
"appId"	INT	4	0~0x0F 默认为 0	
响应				
"ret"	INT	4		错误码

代码参考: action/emv/ActionStoreEmvParams.java

3.3.3. PINPAD 操作

3.3.3.1. 加载密钥

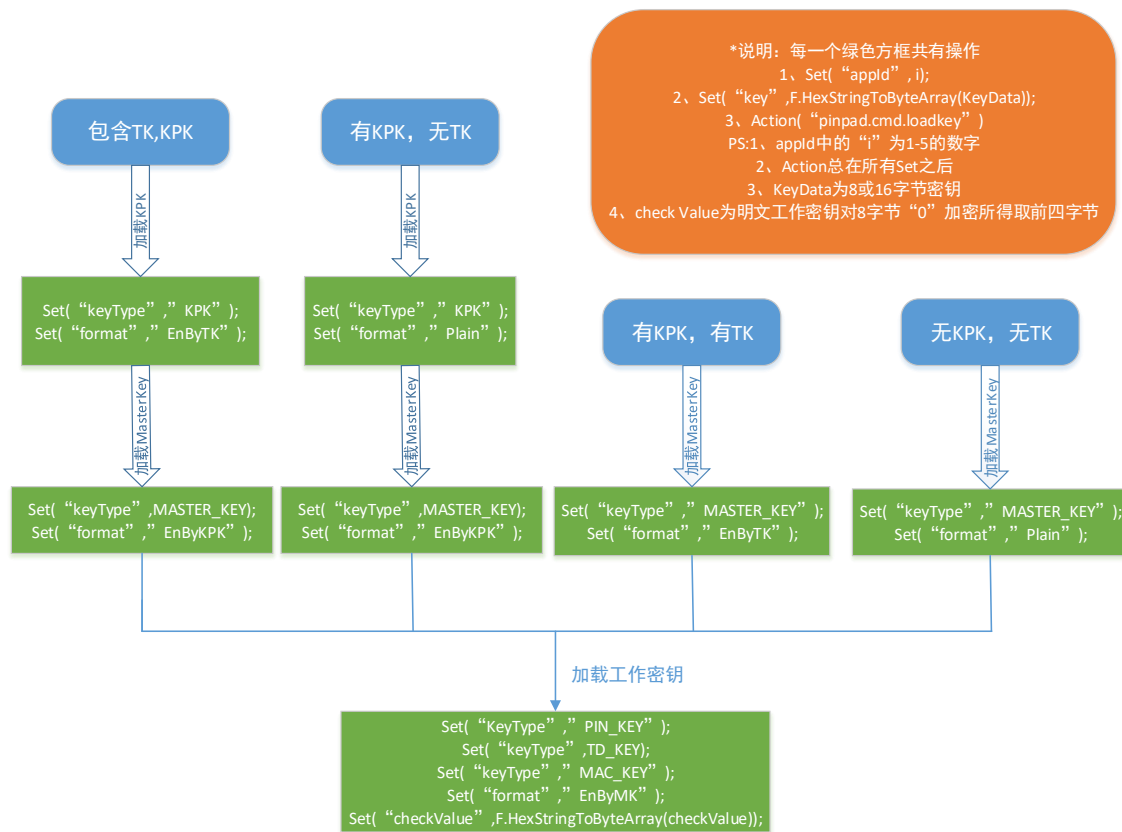
指令: "pinpad.cmd.loadkey"

参数列表:

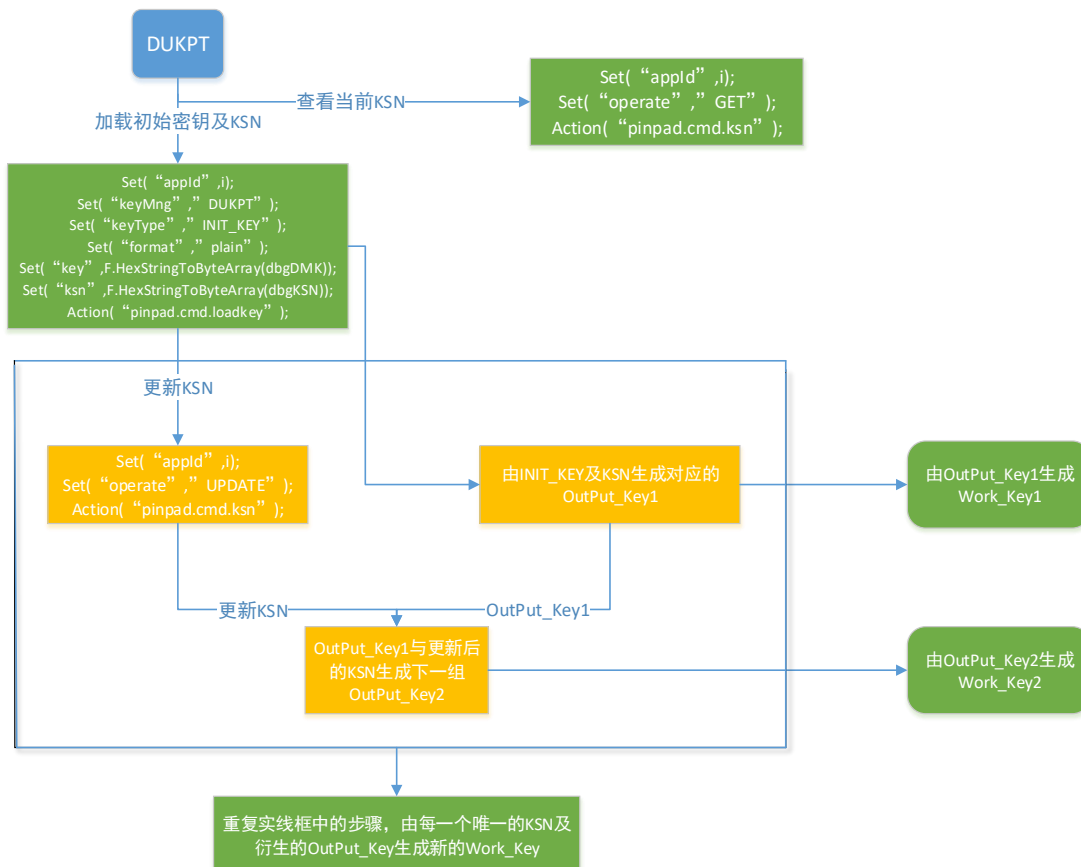
参数名	类型	长度	有效取值/默认值	描述
请求				
"appId"	INT	4	0x01~0x0F 默认 0x01	
"keyMng"	STR	VAR	"MKSK" (默认) "DUKPT" 一次一密 "FIXED" 固定密钥 "JF" 即富定制	密钥管理体系
"keyType"	STR	VAR	"KPK" 传输密钥	密钥类型
			"MASTER_KEY" 主密钥	
			"PIN_KEY" PIK	
			"MAC_KEY" MAK	
			"TD_KEY" TDK	
			"INIT_KEY" DUKPT 的初始密钥	
"format"	STR	VAR	"plain" 明文	密钥数据格式
			"EnByTK" 终端密钥加密	
			"EnByKPK" KPK 加密	
			"EnByMK" 主密钥加密	
			"TR31"	
"key"	BIN	8/16		密钥数据
"checkValue"	BIN	4		密钥校验值 (可选)
"ksn"	BIN	VAR	"DUKPT" 或 "JF" 体系的初始 KSN	仅密钥体系 "DUKPT" 或 "JF" 时存在
响应				
"ret"	INT	4		错误码
"result"	STR	VAR		错误描述

代码参考: action/pinpad/ActionLoadKpk.java、ActionLoadMkey.java 和 ActionLoadWkey.java

MK/SK 秘钥加载流程图:



DUKPT 秘钥加载及原理:



3.3.3.2. 输密码

指令: "pinpad.cmd.pinprocess"

参数列表:

参数名	类型	长度	有效取值/默认值	描述
请求				
"pan"	STR	VAR		主帐号 (可选)
"amount"	STR	VAR		交易金额 (可选)
"keyMng"	STR	VAR	"MKSK" (默认) "DUKPT"一次一密 "FIXED"固定密钥	密钥管理体系
"pinFormat"	STR	VAR	"FORMAT0" (默认) "FORMAT1", "FORMAT3", "PLAIN_TEXT"	PINBLOCK 格式
"noPinFormat",	STR	VAR	"ZERO" (默认) 返回全 0 "PINBLOCK"返回 pinblock	对于无密码的银行卡, 直接按确认时, 是否进行 PINBLOCK 计算
"appId"	INT	4	0x01~0x0F 默认 0x01	
"timeout"	INT	4	10~120 默认 60	单位秒
"pinMinLen"	INT	4	4~12 默认 4	密码最短长度
"pinMaxLen"	INT	4	4~12 默认 12	密码最长长度
响应				
"ret"	INT	4		错误码
"result"	STR	VAR		错误描述
"pinBlock"	BIN	8		

代码参考: action/pinpad/ActionGetPin.java

3.3.3.3. 加解密

指令: "pinpad.cmd.crypto"

参数列表:

参数名	类型	长度	有效取值/默认值	描述
请求				
"operate"	STR	VAR	"ENCRYPT"、"DECRYPT"	
"algorithm"	STR	VAR	"DES_ECB"	加解密算法
"padding"	STR	VAR	"NULL"	不补位
			"M1"	补全 0
			"M2"	补 80 00[n]
"appId"	INT	4	0x01~0x0F 默认 0x01	
"keyMng"	STR	VAR	"MKSK" (默认) "DUKPT"一次一密 "FIXED"固定密钥	密钥管理体系
"keyType"	STR	4	默认"TD_KEY"	
"data"	BIN	VAR		长度 3K 以内
响应				
"ret"	INT	4		错误码
"result"	STR	VAR		错误描述

"data"	BIN	VAR		计算结果
--------	-----	-----	--	------

代码参考: action/pinpad/ActionTestCrypt.java

3.3.3.4. 计算 MAC

指令: "pinpad.cmd.mac"

参数列表:

参数名	类型	长度	有效取值/默认值	描述
请求				
"macType"	STR	VAR	"X99"	
			"ECB"	
			"Unionpay_ECB"	银联算法
			"RICOM"	瑞康定制
"keyMng"	STR	VAR	"MKSK" (默认) "DUKPT" 一次一密 "FIXED" 固定密钥	密钥管理体系
"appId"	INT	4	0x01~0x0F 默认 0x01	
"data"	BIN	VAR		长度 3K 以内
响应				
"ret"	INT	4		错误码
"result"	STR	VAR		错误描述
"mac"	BIN	8/16		

代码参考: action/pinpad/ActionCalculateMac.java

3.3.3.5. 随机数生成

指令: "pinpad.cmd.random"

参数列表:

参数名	类型	长度	有效取值/默认值	描述
请求				
"length"	INT	4	1~3072	要取随机数的长度
响应				
"ret"	INT	4		错误码
"result"	STR	VAR		错误描述
"data"	BIN	VAR		读取的随机数

代码参考: action/pinpad/ActionGetRandom.java

3.3.3.6. 读取/更新 KSN

指令: "pinpad.cmd.ksn"

参数列表:

参数名	类型	长度	有效取值/默认值	描述
请求				
"operate"	STR	VAR	"GET" (默认) 读取当前 KSN "UPDATE" 更新 KSN	目前仅对 DUKPT 密钥体系有效
"appId"	INT	4	0x01~0x0F 默认 0x01	
响应				
"ret"	INT	4		错误码

"result"	STR	VAR		错误描述
"ksn"	BIN	VAR		当前或更新后的 KSN

代码参考: action/pinpad/ActionGetKsn.java 和 action/pinpad/ActionUpdateKsn.java

3.3.3.7. 敏感信息确认

指令: "pinpad.cmd.confirm"

参数列表:

参数名	类型	长度	有效取值/默认值	描述
请求				
"dataType"	STR	VAR	"BALANCE" "TEXT"	余额确认
"data"	STR	VAR		要显示的内容
"data2"	STR	VAR		当 dataType 为 TEXT 时, 第二行显示的内容。
"timeout"	INT	4	10~120 默认 60	单位秒
响应				
"ret"	INT	4		错误码
"result"	STR	VAR		错误描述

代码参考: action/pinpad/ActionDispBalance.java

3.3.3.8. 数字签名

指令: "pinpad.mpr.handwrite"

参数列表:

参数名	类型	长度	有效取值/默认值	描述
请求				
无				
响应				
"ret"	INT	4		错误码
"result"	STR	VAR		错误描述
"fileLen"	INT	4		Bmp 图片文件长度

代码参考: action/pinpad/ActionHandWrite.java

3.3.4. 文件存储

3.3.4.1. 保存文件

指令: "storage.mpw.write_file"

参数列表:

参数名	类型	长度	有效取值/默认值	描述
请求				
"fileType"	STR	VAR	"CERT", "TEXT", "BIN"	文件类型
"fileName"	STR	VAR	长度限在 63 字节内	文件名
"filePath"	STR	VAR		文件路径
"fileData"	BIN	VAR		文件数据(数据和路径二选一)
响应				
"ret"	INT	4		错误码
"result"	STR	VAR		错误描述

* "filePath"和"fileData"两参数必须有 1 个

代码参考：action/storage/ActionStoreFile.java 和 ActionStoreFile2.java

3.3.4.2. 读取文件

指令："storage.mpr.read_file"

参数列表：

参数名	类型	长度	有效取值/默认值	描述
请求				
"fileType"	STR	VAR	"CERT", "TEXT", "BIN"	文件类型
"fileName"	STR	VAR	长度限在 63 字节内	文件名
响应				
"ret"	INT	4		错误码
"result"	STR	VAR		错误描述
"fileData"	BIN	VAR		文件数据

代码参考：action/storage/ActionReadFile.java

3.3.4.3. 删除文件

指令："storage.cmd.delete_file"

参数列表：

参数名	类型	长度	有效取值/默认值	描述
请求				
"fileType"	STR	VAR	"CERT", "TEXT", "BIN", "ALL"	文件类型
"fileName"	STR	VAR	长度限在 63 字节内	文件名
响应				
"ret"	INT	4		错误码
"result"	STR	VAR		错误描述

* 当"fileType"和"fileName"都为"ALL"时，将删除所有文件（初始化文件存储区域）

代码参考：action/storage/ActionDeleteFile.java

3.3.4.4. 保存图片（Bitmap）

指令："storage.mpw.load_bitmap"

参数列表：

参数名	类型	长度	有效取值/默认值	描述
请求				
"type"	STR	VAR	"NORMAL"（默认）	常规轮播用图
			"LOGO"	待机 Logo 图
"index"	INT	4		图 片 索 引 ， 仅 type 为"NORMAL"时需要
"filePath"	STR	VAR		文件路径
"fileData"	BIN	VAR		文件数据(数据和路径二选一)
响应				
"ret"	INT	4		错误码
"result"	STR	VAR		错误描述

* "filePath"和"fileData"两参数必须有 1 个

代码参考: action/storage/ActionStoreBitmap.java 和 ActionStoreLogo.java

3.3.4.5. 加载 EMV 参数

指令: "storage.cmd.load_emvparams"

参数列表:

参数名	类型	长度	有效取值/默认值	描述
请求				
"operate"	STR	VAR	"ADD" (默认)	加载参数
			"CLEAN"	清除参数
"appId"	INT	4	0x01~0x0F 默认 0x01	应用支持多个 APP ID
"type"	STR	VAR	"TERM", "AID", "CAPK", "CARD", "CERT"	参数类型
"data"	BIN	VAR		当"operate"为"ADD"时需要
响应				
"ret"	INT	4		错误码
"result"	STR	VAR		错误描述

代码参考: action/storage/ActionStoreEmvParams.java

注: 当 "type" 为 "TERM" 时, 配置的是终端参数, 目前可以配置的为国家代码 (9F1A), 货币代码 (5F2A), 终端性能 (9F33), 数据为 TLV 格式, 例如:

"9F1A0208405F2A0208409F3303E0E8C0"

3.3.5. 屏幕显示

3.3.5.1. 显示待机 Logo

指令: "exscreen.cmd.idle"

参数列表:

参数名	类型	长度	有效取值/默认值	描述
请求				
无				
响应				
"ret"	INT	4		错误码
"result"	STR	VAR		错误描述

代码参考: action/exscreen/ActionDisplayIdle.java

3.3.5.2. 显示轮播图片

指令: "exscreen.cmd.bitmap"

参数列表:

参数名	类型	长度	有效取值/默认值	描述
请求				
"interval"	INT	4	默认 5 秒	图片的间隔时间, 单位秒
"beginIdx"	INT	4		轮播起始图片索引
"palyNum"	INT	4		轮播图片的数量
响应				
"ret"	INT	4		错误码
"result"	STR	VAR		错误描述

代码参考: action/exscreen/ActionImageCarousel.java

3.3.5.3. 显示客户信息

指令: "exscreen.cmd.custom_msg"

参数列表:

参数名	类型	长度	有效取值/默认值	描述
请求				
"data"	BIN	VAR		客户数据, 用'&'表示换行
响应				
"ret"	INT	4		错误码
"result"	STR	VAR		错误描述

代码参考: action/exscreen/ActionDisplayCustomMsg.java

3.3.5.4. 显示二维码

指令: "exscreen.cmd.qrcode"

参数列表:

参数名	类型	长度	有效取值/默认值	描述
请求				
"data"	BIN	VAR		UTF8 格式的字符串
"payType"	STR	VAR	"ALIPAY":带支付宝图标 "WECHATPAY":带微信支付图标	可选项
"Msgdata"	STR	0/40		二维码下方显示的字符 (ASCII)
响应				
"ret"	INT	4		错误码
"result"	STR	VAR		错误描述

代码参考: action/exscreen/ActionDisplayQR.java

3.3.6. 打印操作

3.3.6.1. 缺纸检查

指令: "printer.cmd.paperout"

参数列表:

参数名	类型	长度	有效取值/默认值	描述
请求				
无				
响应				
"ret"	INT	4		错误码
"result"	STR	VAR		错误描述

代码参考: action/printer/ActionPrintCheckpaper.java

3.3.6.2. 打印文字

指令: "printer.cmd.text"

参数列表:

参数名	类	长	有效取值/默认值	描述
请求				
"data"	STR	VAR		打印内容

"size"	INT	4	大于 0，默认为 24	字体大小
"fonttype"	INT	4	android.graphics.Typeface.NORMAL（默认）	正常
			android.graphics.Typeface.BOLD	粗体
			android.graphics.Typeface.ITALIC	<i>斜体</i>
			android.graphics.Typeface.BOLD_ITALIC	<i>粗斜体</i>
"linegap"	INT	4	大于 0，默认为 6	行间距
"leftmargin"	INT	4	大于等于 0，默认为 0	页左边距
"rightmargin"	INT	4	大于等于 0，默认为 0	页右边距
"typeface"	STR	VAR	如："/mnt/sdcard/kaiti.ttf"（可选）	自定义字体文件路径
响应				
"ret"	INT	4		错误码
"result"	STR	VAR		错误描述

代码参考：action/printer/ActionPrintText.java

3.3.6.3. 走纸

指令："printer.cmd.feed"

参数列表：

参数名	类型	长度	有效取值/默认值	描述
请求				
"lines"	INT	4		走纸行数
响应				
"ret"	INT	4		错误码
"result"	STR	VAR		错误描述

代码参考：action/printer/ActionPrintText.java

3.3.6.4. 打印一维码

指令："printer.cmd.obcode"

参数列表：

参数名	类型	长度	有效取值/默认值	描述
请求				
"data"	STR	VAR		打印内容
响应				
"ret"	INT	4		错误码
"result"	STR	VAR		错误描述

代码参考：action/printer/ActionPrintObcode.java

3.3.6.5. 打印二维码

指令："printer.cmd.qrcode"

参数列表：

参数名	类型	长度	有效取值/默认值	描述
请求				
"data"	STR	VAR		打印内容
响应				
"ret"	INT	4		错误码

"result"	STR	VAR		错误描述
----------	-----	-----	--	------

代码参考: action/printer/ActionPrintQrcode.java

3.3.6.6. 打印图片

指令: "printer.cmd.photo"

参数列表:

参数名	类型	长度	有效取值/默认值	描述
请求				
"data"	Bitmap	VAR		图片数据
响应				
"ret"	INT	4		错误码
"result"	STR	VAR		错误描述

代码参考: action/printer/ActionPrintPhoto.java

3.3.6.7. 等待打印结束

指令: "printer.cmd.busy"

参数列表:

参数名	类型	长度	有效取值/默认值	描述
请求				
响应				
"ret"	INT	4		错误码
"result"	STR	VAR		错误描述

Reference Code: action/printer/ActionPrintBusy.java

3.3.7. 串口操作

3.3.7.1. 打开串口

指令:"usbserial.cmd.serialopen"

参数名	类	长度	有效取值/默认值	描述
请求				
"serialconfig"	STR	VAR	如:"115200,n,8,1"(可选)	串口初始化参数(波特率, 校验位, 数据位, 停止位,)
响应				
"ret"	INT	4		错误码
"result"	STR	VAR		错误描述

代码参考: action/serial/ActionOpen.java

3.3.7.2. 关闭串口

指令:"usbserial.cmd.serialclose"

参数名	类	长度	有效取值/默认值	描述
请求				
无				
响应				
"ret"	INT	4		错误码

"result"	STR	VAR		错误描述
----------	-----	-----	--	------

代码参考: action/serial/ActionClose.java

3.3.7.3. 接受数据

指令:"usbserial.cmd.serialrx"

参数名	类	长度	有效取值/默认值	描述
请求				
maxDataLen	INT	4	大于 0, 小于等于 1024	读取数据的最长长度
Timeout_ms	INT	4	大于 0, 小于等于 10000	读取数据的超时时间(毫秒)
响应				
"ret"	INT	4		错误码
"result"	STR	VAR		错误描述
"data"	BIN	VAR		读到的串口数据

代码参考: action/serial/ActionRx.java

3.3.7.4. 发送数据

指令:"usbserial.cmd.serialtx"

参数名	类	长度	有效取值/默认值	描述
请求				
data	BIN	VAR		发送的串口数据
dataLen	INT	4	大于 0, 小于等于 1024	发送的串口数据长度
响应				
"ret"	INT	4		错误码
"result"	STR	VAR		错误描述

代码参考: action/serial/ActionTx.java

4. 错误码定义

定义	值 (HEX)	值 (DEC)	说明
KV.RET.OK	0x00	0	成功
KV.RET.DATA_ERROR	0x10	16	通讯数据包错误
KV.RET.CMD_ERROR	0x11	17	指令错误
KV.RET.PARAM_ERR	0x12	18	参数错误
KV.RET.FAILED	0x20	32	指令执行失败
KV.RET.BUSY	0x21	33	正在处理其他指令
KV.RET.PROCESSING	0x22	34	指令正在执行中
KV.RET.TIMEOUT	0x23	35	指令执行 (等待) 超时
KV.RET.CANCELED	0x24	36	用户中止操作
KV.RET.EMV_FAILED	0x30	48	EMV 错误
KV.RET.COMMUNICATE_ERROR	0x40	64	通信失败

KV.RET.DEVICE_ERROR	0x50	80	设备异常
KV.RET.OPEN_FAILED	0x51	81	设备打开失败

5. 密钥分配及管理规则

用于说明在 Kivvi 支付终端(Par6、Par10)使用中，每个应用程序（App）的密钥分配、使用规则。

5.1 密钥总数

Kivvi 支付终端(Par6、Par10)共支持存储及使用 15 组相互独立的密钥。

5.2 密钥分配原则

5.2.1 密钥的相互独立性

密钥分配以每个 App 为单位，应用之间互不影响，独立使用自身密钥。

5.2.2 单个 App 密钥组数

每个 App 可分配 0-5 组密钥，最少为不分配，最多分配 5 组。若分配一组，则 AppID 为“1”；若分配两组，则 AppID 为“1”和“2”；以此类推。

5.2.3 密钥的起始位置

每个 App 若至少分配了一组密钥，则其在存储及使用中 AppID 都是从“1”开始的，若两个应用使用了相同 AppID，实际不是同一个，互不影响。例如：A 应用与 B 应用均分配了至少一个 AppID，而在存储及加载时，A 和 B 均使用了 AppID = 1，他们之间是独立使用的。

5.2.4 权限与密钥分配

只有当在 AndroidManifest.xml 中添加 pinpad 操作权限时，软件安装完毕后系统才会弹出对应用 appId 的分配界面，权限获取代码：<uses-permission android:name="adnroid.permission.KIVVI_PINPAD"/>