

高速公路区域联网不停车收费示范工程暂行技术要求 第 9 部分

# 非现金支付卡交易流程规范

2008 年 8 月



## 目 次

1 范围.....	2
2 ICC—PSAM 交易流程概述.....	2
3 复合消费交易流程.....	2
3.1 封闭式入口消费交易流程.....	2
3.2 封闭式出口消费交易流程.....	3
4 传统消费交易流程.....	3
4.1 储值卡/记帐卡的封闭式入口消费交易流程.....	4
4.2 储值卡封闭式出口消费交易流程.....	5
4.3 记帐卡封闭式出口消费交易流程.....	5

## 1 范围

本规范规定了高速公路电子收费系统中用户 IC 卡（包括储值卡和记账卡）与 PSAM 卡之间的消费交易流程。

## 2 ICC—PSAM 交易流程概述

本交易流程规范包含：

- 符合 PBOC 1.0 的 ICC—PSAM 传统消费交易流程。
- 符合 PBOC 2.0 电子钱包扩展应用规范的 ICC—PSAM 复合消费交易流程。

当采用复合消费交易模式时，储值卡和记帐卡采用相同的文件格式和交易流程。记帐卡在封闭式入口的交易中做消费金额为零的复合消费交易，在封闭式出口及开放式收费站完成实际金额的复合消费交易，从“虚拟”钱包中扣款。（“虚拟”钱包中的余额无实际含义，建议以分为单位）。

当采用传统消费交易模式时，记账卡的封闭式出口及开放式消费交易同样需要计算TAC，以MAC计算的方式实现。TAC计算信息域参照电子钱包的TAC，其中不包含“终端机交易序号”。

## 3 复合消费交易流程

### 3.1 封闭式入口消费交易流程

封闭式入口消费交易流程见表4。

表1 复合消费交易封闭式入口消费交易流程

用户 IC 卡		路侧终端		PSAM 卡	备注
卡片复位	←	复位用户卡			
进入 1001 目录	←	选择 1001 目录			从返回的 FCI 里面可以获取 IC 卡卡号等信息，不必再去 0015 文件读取。
	←	读 0019 文件			
返回 0019 文件	→	获得 0019 文件内容			
	←	取钱包余额			
返回电子钱包余额	→	获得钱包余额			
	←	发送复合消费初始化命令，交易金额为 0			
处理复合消费初始化命令	→	得到返回的随机数			
			←	计算 MAC1	
	←	发送更新复合应用数据缓存命令			参见 PBOC2.0
处理更新复合应用数据缓存命令	→				
	←	发送复合消费命令			
验证 MAC1，如果正确则进行交易处理，并返回 TAC 和	→				

MAC2					
		送 MAC2 给 PSAM 校验	→	验证 MAC2	更新终端交易序号文件
		接收校验结果	←	返回校验结果	
卡片复位	←	复位用户卡			

### 3.2 封闭式出口消费交易流程

封闭式出口消费交易流程见下表。

表2 复合消费交易封闭式出口消费交易流程

用户 IC 卡		路侧单元		PSAM 卡
卡片复位	←	复位用户卡		
进入 1001 目录	←	选择 1001 目录,并从 FCI 获得卡号等信息		
	←	读 0019 文件		
返回 0019 文件	→	获得 0019 文件内容 车道机计算通行费额		
	←	取钱包余额		
返回电子钱包余额	→	获得钱包余额		
	←	发送复合消费初始化命令		
处理复合消费初始化命令	→	得到返回的随机数		
			←	计算 MAC1
	←	发送更新复合应用数据缓存命令		
处理更新复合应用数据缓存命令	→			
	←	发送复合消费命令		
验证 MAC1, 如果正确则进行交易处理, 并返回 TAC 码和 MAC2	→			
		MAC2 送 PSAM 进行校验	←	校验 MAC2 及更新终端交易序号文件
		接收 MAC2 校验结果		
卡片复位	←	复位用户卡		

## 4 传统消费交易流程

### 4.1 储值卡 / 记账卡的封闭式入口消费交易流程

储值卡 / 记账卡的封闭式入口消费交易流程见表1。

表3 储值卡 / 记账卡的封闭式入口消费交易流程

用户 IC 卡		路侧终端		PSAM 卡	备注
---------	--	------	--	--------	----

卡片复位	←	复位用户卡			
进入 1001 目录	←	选择 1001 目录			从返回的 FCI 里面 可 以 获 取 PBOC 2.0 标准的 0015 文件内容。
返回 0015 文件	→	获得 IC 卡卡号等信息			
	←	读 0012 文件			
返回 0012 文件	→	获得 0012 文件			
	←	读 0002 文件			记账卡无此步骤
返回 0002 文件	→	获得钱包余额			记账卡无此步骤
		取随机数	→		内部认证过程
			←	返回取随机数	
内部认证加密运算	←	送随机数进行内部认证			
返回加密结果	→				
		DES 运算初始化	→	计算过程密钥	
		对随机数进行加密	→	加密运算	
		对卡片内部认证	←	返回加密结果	
	←	取随机数			外部认证过程
返回取随机数	→				
		DES 运算初始化	→	计算过程密钥	
		对随机数进行加密	→	加密运算	
			←	返回加密结果	
进行认证计算	←	外部认证			
返回认证结果	→				
	←	写 0012 文件			
返回写入结果	→				
卡片复位	←	复位用户卡			

#### 4.2 储值卡的封闭式出口消费交易流程

储值卡的封闭式出口消费交易流程见表2。

表4 储值卡的封闭式出口消费交易流程

用户 IC 卡		路侧单元		PSAM 卡
卡片复位	←	复位用户卡		
进入 1001 目录	←	选择 1001 目录		从返回的 FCI 里面可以获取 PBOC 2.0 标准的 0015 文件内容。
返回 0015 文件	→	获得 IC 卡卡号等信息		
	←	读 0012 文件		
返回 0012 文件	→	获得 0012 文件		
	←	读 0002 文件		
返回 0002 文件	→	获得钱包余额		
		车道机计算通行费额		

用户 IC 卡		路侧单元		PSAM 卡
	←	消费交易初始化命令		
返回初始化结果	→			
		计算 MAC1	→	
			←	返回 MAC1
	←	消费交易		
返回 TAC 和 MAC2	→	接收 TAC		
		送 MAC2 给 PSAM 校验	→	校验 MAC2 并更新终端交易序号文件
		接收校验结果	←	返回校验结果
	←	取随机数		
返回取随机数	→			
		DES 运算初始化	→	计算过程密钥
		对随机数进行加密	→	加密运算
			←	返回加密结果
进行认证计算	←	外部认证		
返回认证结果	→			
	←	写 0012 文件		
返回写入结果	→			
卡片复位	←	复位用户卡		

#### 4.3 记账卡封闭式出口消费交易流程

记帐卡封闭式出口消费交易流程见表3。

表5 记账卡的封闭式出口消费交易流程

用户 IC 卡		路侧终端		PSAM 卡	备注
卡片复位	←	复位用户卡			
进入 1001 目录	←	选择 1001 目录			从返回的 FCI 里面可以获取 PBOC 2.0 标准的 0015 文件内容。
返回 0015 文件	→	获得 IC 卡卡号等信息			
	←	读 0012 文件			
返回 0012 文件	→	获得 0012 文件			
		计算通行费额			
		取随机数	→		内部认证过程
			←	返回取随机数	
内部认证加密运算	←	送随机数进行内部认证			
返回加密结果	→				
		DES 运算初始化	→	计算过程密钥	
		对随机数进行加密	→	加密运算	
		对卡片内部认证	←	返回加密结果	

	←	取随机数			外部认证过程
返回取随机数	→				
		DES 运算初始化	→	计算过程密钥	
		对随机数进行加密	→	加密运算	
			←	返回加密结果	
进行认证计算	←	外部认证			
返回认证结果	→				
	←	写 0012 文件			
返回写入结果	→				
	←	计算 TAC			
返回 TAC	→				
卡片复位	←	复位用户卡			