中国石化卡机联动加油机
安全提升标准 V2.4

（送审稿）

2011-××-××发布　　2011-××-××实施

中国石油化工股份有限公司 发布

目　　录

前 言

截止到 2010 年，《中国石化加油集成电路（IC）卡应用规范》V2.0 由以下 3 部分组成：

——接触式 IC 卡接口规范；

——非接触 IC 卡射频接口规范；

——加油卡 COS 及应用规范。

考虑到加油卡应用的延续以及方便规范文本管理，于 2011 年将《卡机联动加油机安全提升标准》纳入《中国石化加油集成电路（IC）卡应用规范》V2.0 体系，并将其作为规范的第 4 部分。

本部分在《中国石化加油集成电路（IC）卡应用规范》（V2.0）其他部分基础上制定而成。

本部分由中国石化销售有限公司提出。

本部分由中国石油化工股份有限公司归口管理。

本部分主要起草单位：

中国石化销售有限公司

本部分主要起草人：

引 言

《卡机联动加油机安全提升标准》制定的目的是，通过应用先进技术与配套管理手段，防止非正常改动加油机程序，从而提升卡机联动加油机设备安全，为加强加油站生产管理和保障加油站平稳运营等提供有效措施，同时也可为其它同类应用工程提供指导和借鉴。

本标准适用范围和对象:中国石化加油卡工程——IC 卡加油的卡机联动加油机。

本标准包括以下主要内容:

—卡机联动加油机安全提升原理描述。描述了安全机制原理、概念等。

—卡机联动加油机安全提升操作规程。描述了 PSAM 卡和加油机终端之间的处理流程，指令等。

—卡机联动加油机安全提升管理与保障措施。给出了安全体系涉及的配套卡片及相关操作流程、建议等。

1　加油机安全提升概述

1.1　原理描述

（1）对加油机计量芯片实施身份号码管理，身份号码由厂商代码和芯片生产序列号组成，具备唯一性（简称芯片 ID）。

（2）加油机计量芯片内存储与芯片 ID 对应的身份验证密钥，身份密钥具备唯一性。

（3）加油 PSAM 卡存储其宿主加油机的计量芯片身份验证密钥，与计量芯片一一对应，相互绑定，实现“一片一密”。

（4）加油 IC 卡插卡加油时，加油机 IC 卡 POS 在对加油卡执行置灰命令操作前，先对“加油机计量芯片”进行身份验证，验证通过，继续加油卡操作；否则，POS 停止操作并报警（显示“计量芯片验证失败”），同时：(a) 加油 PSAM 内计量芯片认证计数器增一，当失败计数连续增加到 50 时，加油 PSAM 锁死；(b) POS 读取 PSAM 内计量芯片认证计数器数值，生成报警信息后通过石化通讯协议的加油机出错命令传给后台管控机。

（5）加油机管控机存储加油机计量芯片注册（成功或失败）、身份验证失败操作日志（日志报文格式见数据元 9.3 部分），便于后期集中监控应用扩展。

1.2　安全机制

（1）引入加油机生产商、油机使用者（油站）、业务管理部门（油站上级管理部门）三方协作、制约机制，科学合理、可操作性强，形成安全闭环，强化管理与监督。

（2）石化省市业务管理部门掌管加油 PSAM 与计量芯片绑定操作的授权卡（简称 ACT 卡），监督油机现场装机/维护操作，授权加油 PSAM 卡启动“一片一密”之密钥配置工作。ACT 卡由省市分公司统一制卡、领用，安排专人管理使用。

（3）加油机生产商现场服务人员掌管本厂生产加油机计量芯片的密钥配置与注册卡（简称 RID 卡），执行油机现场装机/维护操作，实施计量芯片向加油 PSAM 卡的注册及密钥配置工作。加油机出厂时即灌装好该计量芯片身份密钥，计量芯片具有唯一编号（ID），不同编号的计量芯片，其身份密钥不同。

（4）中石化总部负责管理加油机计量芯片身份根密钥及加油 PSAM 与计量芯片绑定授权身份根密钥。

1.3　应用特点

（1）加油 PSAM 卡内电子油票和积分应用密钥维持原有体系，没有改变，也不受任何影响。

（2）即使 IC 卡 POS 由于某种原因不能成功执行、甚至跳过加油机计量芯片身份验证环节，即在加油 PSAM 没有成功验证计量芯片身份的情况下而强行加油，则加油 PSAM 将拒绝提供后续的加油卡灰锁、扣

款、解灰等密钥服务，从而导致用户（消费者）不能使用加油 IC 卡支付购油。

2　安全提升机卡操作规程

2.1 PSAM 卡预处理

本段所述 PSAM 卡预处理过程仅给出了安全提升目的所涉及的操作，对于正常卡机联动加油交易处理所描述的内容请参照《中国石化加油 IC 卡规范》。

a) 加油机对 PSAM 卡上电复位；

b) 读取 PSAM 卡卡号等数据；

c) 选择中石化应用 1；

d) 读取 PSAM 卡内应用接收方标识、起始日期和有效日期，并进行相关合法性判断；当前时间到达 PSAM 卡有效日期失效前 3 个月内，加油机上下班时应当提示“PSAM 卡有效期至　XXXX 年 XX 月 XX 日，请更换 PSAM 卡”　。

e) 执行 GET ANTI-PLAGIAREZE PROOF（获取安全提升启用状态）命令，可能返回的状态码有:(1) 状态码‘6D00’或‘9B01’ 表示“PSAM 卡安全提升功能失效，应提示“请更换 PSAM 卡”；(2) 状态码‘9B02’表示“芯片未注册”，此情下加油机应当停止加油服务,先进行芯片注册处理；(3) 状态码‘9B03’ 表示安全提升密钥已经锁定，此情下加油机应提示“安全锁定，请更换 PSAM 卡或重新绑定”；(4) 状态码‘9000’及 1 字节数据’XX’ ,XX∈[1,255]，表示命令执行成功，说明安全提升功能已经启用，此情下加油机应提示:“身份验证剩 XX 次机会”。

2.2 ACT 卡处理流程

当加油机安装的 PSAM 卡支持安全提升功能时，插入 ACT 卡后进入本处理流程，否则提示“请更换 PSAM 卡”。

当加油机插入 ACT 卡后，执行如下流程：

a) 加油机对 ACT 卡上电复位；

b) 选择中石化应用；

c) 读取 ACT 卡内的发卡方标识、起始日期、有效日期、ACT 卡号，并进行相关合法性判断；

d) 合法性检查的内容包括 PSAM 卡接收方标识与 ACT 卡发卡方标识是否一致，ACT 卡是否过有效期。

e) 读取 ACT 卡内的‘认证密钥索引号’。

f) 输入个人 PIN

g) 油机向 PSAM 卡申请随机数。

h) 油机向 ACT 卡发送 DES CRYPT 命令，对随机数进行加密，其中 P2 为 ACT 卡指定的“认证密钥索引号”,获取加密数据。

i) 油机向 PSAM 卡发送 START BINDING SERVICE 命令。命令中包含上步骤加密数据，P1 为 ACT 卡‘认证密钥索引号’。

j) PSAM 卡认证成功并返回状态码’9000’后，油机应提示“ACT 成功，请插入 RID 卡（建议油机只在此时机实现接受并处理 RID 卡的流程)”，如果插入 RID 卡则进入”RID 卡处理流程”，若不是 RID 卡，则退出；PSAM 卡认证失败，返回其他状态码，油机应提示“ACT 失败”，退出。

2.3 RID 卡处理流程

当加油机所安装的 PSAM 卡进入“ACT 成功，请插入 RID 卡”状态，RID 卡插入油机后进入本处理流程，否则油机提示“ACT 未启动”。

当加油机插入 RID 卡后，执行如下流程：

a) 加油机对 RID 卡上电复位；

b) 选择中石化应用；

c) 读取 RID 卡内的油机厂商标识、起始日期、有效日期、RID 卡号，并进行相关合法性判断；

d) 合法性检查的内容包括芯片内存储的油机厂商标识与 RID 卡内的油机厂商标识是否一致，RID 卡是否过有效期。

e) 读取 RID 卡‘认证密钥索引号’和‘计算密钥版本号’。

f) 输入个人 PIN

g) 油机向 PSAM 卡申请随机数。

h) 油机向 RID 卡发送 DES CRYPT 命令，对随机数进行加密，其中 P2 为 RID 卡指定的“认证密钥索引号” ，获取加密数据。

i) 油机向 PSAM 卡发送 INIT_SAM_BINDING 命令，将加密数据送入 PSAM 卡进行认证。在该命令中 P1 为 RID 卡‘认证密钥索引号’。

j) INIT_SAM_BINDING 命令成功后，油机获取计量芯片 ID，并向 PSAM 卡发送 SAM_BINDING 命令，并提示“正在注册，请等待”; INIT_SAM_BINDING 命令失败，油机应提示“RID 验证失败，请

重新插入 RID 卡”，如果重新插入 RID 卡则重新进入本处理流程。

k) SAM_BINDING 命令成功后，产生操作日志；后续步骤 i-iii 给出了产生操作日志的方法。

i. 油机向 PSAM 卡发送 INIT__FOR__DESCRYPT 命令，其中 P2 为 RID 卡指定的“加密密钥版本号” ，启动日志数据 MAC 计算。

ii. 油机向 PSAM 卡发送 DES CRYPT 命令，对如下数据计算 MAC：

启动绑定日期时间（7 字节）

ACT 卡卡号（10 字节）

ACT 卡认证密钥索引（1 字节）

RID 卡卡号（10 字节）

RID 卡认证密钥索引（1 字节）

日志 MAC 计算密钥索引（1 字节）

PSAM 卡卡号（10 字节）

油机芯片 ID（8 字节）

iii. 油机向 RID 卡发送 APPEND LOG RECORD 命令更新日志记录，日志记录包含如下数据：

启动绑定日期时间（7 字节）

ACT 卡卡号（10 字节）

ACT 卡认证密钥索引（1 字节）

RID 卡卡号（10 字节）

RID 卡认证密钥索引（1 字节）

日志 MAC 计算密钥索引（1 字节）

PSAM 卡卡号（10 字节）

油机芯片 ID（8 字节）

MAC(4 字节)

l)产生操作日志完毕后，加油机计量芯片注册完毕，加油机应提示“芯片注册成功”，油机可以进入正常加油功能；若 SAM_BINDING 命令失败，则提示“芯片注册失败”，退出。

2.4 加油前身份验证流程

加油机计量芯片成功完成注册后，当插入 IC 卡（加油用户卡、员工卡、验泵卡和维修卡）时，油机执行《中国石化加油 IC 卡应用规范》中规定的交易预处理流程后、执行 INIT_SAM_GREY_LOCK 命令前，执行本段流程。

加油前身份验证流程：

a) 油机向 PSAM 卡申请随机数；

b) 油机向计量芯片发送加密随机数命令，获得加密结果；

c) 油机向 PSAM 卡发送 ANTI-PLAGIAREZE AUTHENTICATION 命令，认证计量芯片合法性。如果 PSAM 卡返回’9000’,表示芯片身份合法，继续下一步。否则，根据相应状态码给出提示后停止加油操作。

d) 油机向 PSAM 卡发送 INIT_SAM_GREY_LOCK（计算 MAC1）命令开始正常加油流程……

3　PSAM 卡提升专用指令集

本部分所定义的指令是在《中石化加油 IC 卡规范 V1.0》第 5 部分基础上，增加了安全提升专用指令。

3.1　GET ANTI-PLAGIAREZE PROOF 命令

3.1.1　定义和范围

GET ANTI-PLAGIAREZE PROOF 命令用于获取安全提升功能启用状态。

3.1.2　命令报文

GET ANTI-PLAGIAREZE PROOF 命令报文见表 3－1。

表 3－1　GET ANTI-PLAGIAREZE PROOF 命令报文

代码	值
CLA	80h
INS	A2h
P1	00h
P2	00h
Lc	不存在
Data	不存在
Le	00

3.1.3　命令报文数据域

命令报文数据域不存在。

3.1.4　响应报文数据域

该命令成功执行，响应报文数据域定义见表 3-2。

表 3-2　GET ANTI-PLAGIAREZE PROOF 响应报文数据域

值	含义
XX	安全功能已启用，身份认证还剩 XX 次机会

3.1.5　响应报文的状态码

执行成功返回 9000。　表 3－3 为错误状态码。

表 3－3　GET ANTI-PLAGIAREZE PROOF 命令状态码

SW1	SW2	含义
9B	01	安全功能未启用
9B	02	计量芯片未注册
9B	03	安全功能锁定
69	85	使用条件不满足（不在应用下或应用锁定）
6A	86	P1 或 P2 不正确
6D	00	INS 不正确
6E	00	CLA 不正确
93	03	应用被永久锁定

3.2　ANTI-PLAGIAREZE AUTHENTICATION 命令

3.2.1 定义和范围

ANTI-PLAGIAREZE AUTHENTICATION 命令用于启动加油专有消费流程前的安全提升安全认证。计算的方法是利用卡片中的安全提升密钥，对卡片产生的随机数（使用 GET CHALLENGE 命令）和接口设备传输进来的认证数据进行验证。

当 PSAM 卡返回状态码 9000 时，才具备后续执行 INIT_SAM_GREY_LOCK 命令的必要条件。

3.2.2 命令报文

ANTI-PLAGIAREZE AUTHENTICATION 命令报文见表 3－4。

表 3－4　ANTI-PLAGIAREZE AUTHENTICATION 命令报文

代码	值
CLA	80h
INS	AEh
P1	00
P2	00
Lc	08h
Data	认证数据（8 字节）
Le	不存在

3.2.3 命令报文数据域

命令报文数据域中包含 8 字节的认证数据，该数据是用主控密钥对此命令前一条命令“GET CHALLENGE”命令获得随机数后缀“00 00 00 00”之后做 3DES 加密运算产生的。

3.2.4 响应报文数据域

响应报文数据域不存在。

3.2.5 响应报文的状态码

执行成功返回 9000。　表 3－5 为错误状态码。

表 3－5　ANTI-PLAGIAREZE AUTHENTICATION 命令状态码

SW1	SW2	含义
9B	01	安全功能未启用
9B	02	计量芯片未注册
9B	03	安全功能锁定
6B	XX	身份认证失败，剩余 XX 次重试机会
67	00	长度错误（Lc 为空）
69	84	随机数无效
69	85	使用条件不满足（不在应用下或应用被锁定）
6A	86	P1 或 P2 不正确
6D	00	INS 不正确
6E	00	CLA 不正确
93	03	应用被永久锁定

3.3　INIT_SAM_GREY_LOCK 命令

3.3.1 定义和范围

该命令的执行条件是 ANTI-PLAGIAREZE AUTHENTICATION 认证通过。

INIT_SAM_GREY_LOCK 命令用于建立过程密钥并且计算 MAC1。只有成功执行了这条命令才允许执行 CERTIFICATE_SAM_GREY_LOCK（验证 MAC2）命令。这条命令执行成功后 PSAM 卡的状态在 PSAM 卡下电重新上电后仍能恢复，而且建立的过程密钥也是有掉电保持的，只有在下一次执行 INIT_SAM_GREY_LOCK 命令时才被更新。

3.3.2 命令报文

INIT_SAM_GREY_LOCK 命令报文见表 3-6

表 3-6　INIT_SAM_GREY_LOCK 命令报文

代码	值
CLA	‘E0’
INS	‘40’
P1	‘00’
P2	‘00’
L_c	‘14+8*N’　（N=1，2，3）
Data	见表 3-4
L_e	‘0C’

3.3.3 命令报文数据域

表 3-7 定义了命令报文的数据域：

表 3-7　INIT_SAM_GREY_LOCK 命令报文数据域

说明	长度（字节）
用户卡随机数	4
用户卡电子油票脱机交易序号	2
用户卡电子油票余额	4
交易类型标识	1
交易日期（终端）	4
交易时间（终端）	3
密钥版本号（加油消费密钥）	1
密钥算法标识（加油消费密钥）	1
用户卡电子油票应用序列号(最右 16 位数字)	8
成员标识	8
试点城市标识	8

3.3.4 响应报文数据域

此命令执行成功的响应报文数据域见表 3-8。
如果命令执行不成功，则只在响应报文中回送 SW1 和 SW2。
INIT_SAM_GREY_LOCK 响应报文数据域

表 3-8　INIT_SAM_GREY_LOCK 响应报文数据域

说明	长度（字节）
终端交易序号	4
终端随机数	4
MAC1	4

3.3.5 响应报文的状态码

此命令执行成功的状态码是‘9000’。
表 3-9 描述了 IC 卡可能回送的错误状态。

表 3-9　INIT_SAM_GREY_LOCK 错误状态

SW1	SW2	说明
‘9B’	‘06’	未执行安全身份认证
‘64’	‘00’	标志状态位没变
‘65’	‘81’	内存错误
‘67’	‘00’	长度错误
‘69’	‘85’	使用条件不满足（不在应用下或应用被锁定）
‘69’	‘85’	使用条件不满足（应用被锁定）
‘69’	‘86’	不满足命令执行条件（当前文件不是 DF）
‘6A’	‘80’	数据参数不正确（如密钥分散级别与数据不符）
‘6A’	‘86’	P1 或 P2 不正确
‘6A’	‘88’	引用数据未找到
‘6D’	‘00’	INS 不正确
‘6E’	‘00’	CLA 不正确
‘93’	‘03’	应用被永久锁定
‘94’	‘03’	密钥版本不支持

3.4　START BINDING SERVICE 命令

3.4.1 定义和范围

START BINDING SERVICE 命令用于 PSAM 卡获得 ACT 卡授权通过后启动芯片注册服务功能。

当 PSAM 卡片返回状态码为 9000，则芯片注册服务成功启动，可以执行后续 INIT_SAM_BINDING_SERVICE 命令。

如果 PSAM 卡片返回‘9B01’,则表明安全提升功能未启用。

如果 PSAM 卡片返回‘6BCx’,则表明 ACT 授权认证失败，还有 X 次尝试机会，最大尝试次数为 15 次，如果返回 6BC0 则 ACT 授权认证失败，禁止授权。

如果 PSAM 卡片返回‘6983’,则表明 ACT 授权功能锁定。

3.4.2 命令报文

START BINDING SERVICE 命令报文见表 3－10。

表 3－10 START BINDING SERVICE 命令报文

代码	值
CLA	80h
INS	A6h
P1	该数值为 ACT 卡指定的密钥索引号
P2	00h
Lc	10h
Data	ACT 卡卡号（8 字节）+启动服务认证数据
Le	不存在

3.4.3 命令报文数据域

命令报文数据域中包含 8 字节的加密数据，该数据是用主控密钥对此命令前一条命令“GET CHALLENGE”命令获得随机数后缀“00 00 00 00”之后做 3DES 加密运算产生的。

3.4.4 响应报文数据域

响应报文数据域不存在。

3.4.5 响应报文的状态码

执行成功返回 9000。　表 3－11 为错误状态码。

表 3－11　START BINDING SERVICE 命令状态码

SW1	SW2	含义
9B	01	安全功能未启用
6B	Cx	ACT 授权失败，‘x’表示允许重试的次数
67	00	长度错误（Lc 为空）
69	83	认证方法锁定
69	84	随机数无效
69	85	使用条件不满足（不在应用下或应用被锁定）
69	85	使用条件不满足
6A	86	P1 或 P2 不正确
6D	00	INS 不正确
6E	00	CLA 不正确
93	03	应用被永久锁定

3.5　INIT_SAM_BINDING 命令

3.5.1 定义和范围

INIT_SAM_BINDING 命令用于初始化 PSAM 卡以实现油机计量芯片的注册，该指令执行前需要校验 PIN。

执行该指令前终端需先使用 GET CHALLENGE 命令向 PSAM 卡申请随机数。

3.5.2 命令报文

INIT_SAM_BINDING 命令报文见表 3－12。

表 3－12　INIT_SAM_BINDING 命令报文

代码	值
CLA	80h

INS	Ach
P1	该数值为 RID 卡指定的密钥索引号
P2	00h
Lc	18h
Data	RID 卡卡号（8 字节） 油机厂家 ID（8 字节，不足补 FF） 认证数据
Le	不存在

3.5.3 命令报文数据域

命令报文数据域中包含 8 字节的认证数据，该数据是用主控密钥对此命令前一条命令“GET CHALLENGE”命令获得随机数后缀“00 00 00 00”之后做 3DES 加密运算产生的。

3.5.4 响应报文数据域

响应报文数据域不存在。

3.5.5 响应报文的状态码

执行成功返回 9000。　表 3－13 为错误状态码。

表 3－13　INIT_SAM_BINDING 命令状态码

SW1	SW2	含义
9B	01	安全功能未启用
9B	07	未执行 ACT 授权
6B	Dx	RID 身份验证失败，‘x’表示允许重试的次数
67	00	长度错误（Lc 为空）
69	83	认证方法锁定
69	84	随机数无效
69	85	使用条件不满足（不在应用下或应用被锁定）
6A	86	P1 或 P2 不正确
6D	00	INS 不正确
6E	00	CLA 不正确
93	03	应用被永久锁定

3.6　SAM_BINDING 命令

3.6.1 定义和范围

SAM_BINDING 命令用于完成 PSAM 卡和加油机计量芯片的绑定功能。执行该指令前必须成功执行 INIT_SAM_BINDING 指令。

3.6.2 命令报文

SAM_BINDING 命令报文见表 3－14。

表 3－14　SAM_BINDING 命令报文

代码	值
CLA	84h
INS	AAh
P1	00h
P2	00h
Lc	10h
Data	油机芯片身份数据（16 字节）
Le	不存在

3.6.3 命令报文数据域

命令报文为厂家芯片 ID 和油机厂家 ID。

3.6.4 响应报文数据域

响应报文数据域不存在。

3.6.5 响应报文的状态码

执行成功返回 9000。　表 3－15 为错误状态码。

表 3－15　SAM_BINDING 命令状态码

SW1	SW2	含义
9B	01	安全功能未启用
9B	05	厂家 ID 不匹配
9B	08	没有执行 INIT_SAM_BINDING 命令
67	00	长度错误（Lc 为空）
69	84	随机数无效
69	85	使用条件不满足（不在应用下或应用被锁定）
6A	86	P1 或 P2 不正确
6D	00	INS 不正确
6E	00	CLA 不正确
93	03	应用被永久锁定

4　RID卡指令集

4.1　EXPORT LOG RECORD 命令

4.1.1　定义和范围

EXPORT LOG RECORD 命令用于导出日志交易备份文件保存的日志记录。该命令通过指定记录号的方式导出日志记录数据。记录号“01”是最新的一条记录，记录类似一个堆栈，最先写入的记录号最大，最后写入的记录号最小。

站级后台系统可以先通过 GET LOG FILE PARA 命令（参数 P1 为 01）读取尚未导出的记录数的计数器。然后使用本命令设置记录值从 1 递增（记录后入先出）或递减至 1（记录先入先出）的方式连续导出记录。

将未导出记录导出成功之后，可以使用 SET LOG FILE PARA 命令的参数 P1 为 01、命令报文值为 0000，将卡片的未导出记录计数器清 0。

4.1.2　使用条件和安全

EXPORT LOG RECORD 命令的执行必须先验证卡片的 PIN。

4.1.3　命令报文

EXPORT LOG RECORD 命令报文编码见表 3-16：

表 3-16　　EXPORT LOG RECORD 命令报文

代码	值								
CLA	‘80’								
INS	‘B6’								
P1	记录号（记录号的低 8 位）								
P2	B8	b7	b6	b5	b4	b3	b2	b1	说　明
	0	0	0	0	0	1	x	x	记录号高 2 位
Lc	不存在								
DATA	不存在								
Le	期望返回的记录数据								

4.1.4　响应报文数据域

所有执行成功的 EXPORT LOG RECORD 命令的响应报文数据域由读取的指定记录号的日志数据组成。

4.1.5　响应报文状态码

IC 卡可能回送的错误状态码如表 3-17 所示：

表 3-17　　EXPORT LOG RECORD 错误状态

SW1	SW2	含　义
90	00	命令执行成功
65	81	写 EEPROM 失败
67	00	Lc 长度错误
69	82	不满足安全状态
6A	83	未找到记录
6A	86	P1、P2 参数错
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

4.2　APPEND LOG RECORD 命令

4.2.1　定义和范围

APPEND LOG RECORD 命令用于向日志交易备份文件中添加日志记录。

在执行添加日志记录指令时，如果已添加的日志记录个数超过允许值时，会返回错误，终端应通过读取相应的日志记录并对当前的已添加记录个数值设置为 0，以完成日志记录的继续添加。导出日志交易备份文件保存的日志记录。该命令通过指定记录号的方式导出日志记录数据。记录号“01”是最新的一条记录，记录类似一个堆栈，最先写入的记录号最大，最后写入的记录号最小。每成功添加一条记录，未导出记录的计数器就自动加 1。

当前已添加记录个数数值应小于添加记录上限值。

在添加日志记录的过程中，如果过程意外中断，加油机应该使用 EXPORT LOG RECORD 命令（P1=01）先读出最后一笔记录的内容，判断最后一笔记录是否写成功来判断应该从加油机上的哪条日志记录开始继续添加。

4.2.2　使用条件和安全

APPEND LOG RECORD 命令的执行必须先验证卡片的 PIN。

4.2.3　命令报文

APPEND LOG RECORD 命令报文编码见表 3-18：

表 3-18　　APPEND LOG RECORD 命令报文

代码	值
CLA	‘80’
INS	‘E6’
P1	‘00’
P2	‘00’
Lc	DATA 域的长度
DATA	一条日志交易记录数据

Le	不存在

4.2.4 命令报文数据域

命令报文数据域由一条日志交易记录组成。

4.2.5 响应报文数据域

响应报文数据域不存在。

4.2.6 响应报文状态码

IC 卡可能回送的错误状态码如表 3-19 所示：

表 3-19　　APPEND LOG RECORD 错误状态

SW1	SW2	含　义
90	00	命令执行成功
65	81	写 EEPROM 失败
67	00	Lc 长度错误
69	82	不满足安全状态
6A	83	未找到记录
6A	86	P1、P2 参数错
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定
94	07	记录数到达限制值

4.3 GET LOG FILE PARA 命令

4.3.1 定义和范围

GET LOG FILE PARA 命令有两个功能，一个功能是用于获取文件中允许添加记录的上限，另一个功能是获取文件中已添加并且尚未导出的记录个数等参数值（其应该是之前 1 次或几次 SET LOG FILE PARA 的参数 P1 为 01 时的命令报文中记录值的累加，直到 SET LOG FILE PARA 命令的参数 P1 为 01、命令报文值为 0000 时，未导出记录计数器清 0）。

4.3.2 使用条件和安全

GET LOG FILE PARA 命令的执行必须先验证卡片的 PIN。

4.3.3 命令报文

GET LOG FILE PARA 命令报文编码见表 3-20：

表 3-20　　GET LOG FILE PARA 命令报文

代码	数　值
CLA	‘80’
INS	‘B8’
P1	‘00’获取日志交易记录文件的允许添加记录的上限 ‘01’获取日志交易记录文件当前已经添加并且尚未导出的记录个数
P2	00
Lc	不存在
DATA	不存在
Le	‘02’

4.3.4 响应报文数据域

执行成功的 GET LOG FILE PARA 命令的响应报文数据域由读取的日志文件参数组成。两个字节的记录数，最大值 65535，例如返回 0120（16 进制），就是 288 条。

4.3.5 响应报文状态码

IC 卡可能回送的错误状态码如表 3-21 所示：

表 3-21　　GET LOG FILE PARA 错误状态

SW1	SW2	含　义
90	00	命令执行成功
65	81	写 EEPROM 失败
67	00	Lc 长度错误
69	82	不满足安全状态
6A	83	未找到记录
6A	86	P1、P2 参数错
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

4.4　SET LOG FILE PARA 命令

4.4.1 命令描述

SET LOG FILE PARA 命令用于设置日志文件中添加记录上限和将当前未导出记录数的计数器清零。

当前已添加记录个数数值应小于添加记录上限值。

4.4.2 使用条件和安全

SET LOG FILE PARA 命令的执行必须先验证卡片的 PIN。

4.4.3 命令报文

SET LOG FILE PARA 命令报文编码见表 3-22：

表 3-22　　SET LOG FILE PARA 命令报文

代码	数　值
CLA	‘80’
INS	‘BA’
P1	‘00’设置日志记录文件添加记录的上限 ‘01’将最新的已经导出的记录数设置为已导出状态，即清除未导出记录计数器
P2	00
Lc	DATA 域的长度
DATA	两个字节，值域为‘0000’— ‘03FF’ 当 P1=01 时，DATA=‘0000‘表示将未导出记录数清零。其它值无意义
Le	不存在

4.4.4 响应报文数据域

响应报文数据域不存在。

4.4.5 响应报文状态码

此命令执行成功的状态码是‘9000’。
IC 卡可能回送的警告状态码如表 3-23 所示：

表 3-23　　SET LOG FILE PARA 错误状态

SW1	SW2	含　义
90	00	命令执行成功
65	81	写 EEPROM 失败
67	00	Lc 长度错误
69	82	不满足安全状态
6A	83	未找到记录
6A	86	P1、P2 参数错
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

5　ACT/RID卡共有指令集

5.1　APPLICATION　BLOCK 命令

5.1.1 定义和范围

APPLICATION BLOCK 命令使当前选择的应用失效。
当 APPLICATION BLOCK 命令成功地完成后，用 SELECT 命令选择已失效的应用，将回送状态码“选择文件无效”（SW1 SW2＝’6283’）。
对其他命令的影响根据不同应用而定。

5.1.2 命令报文

APPLICATION BLOCK 命令报文编码见表 3-24：
表 3-24　　APPLICATION BLOCK 命令报文

代码	值
CLA	’84’
INS	‘1E’
P1	‘00’，其他值保留为将来使用
P2	‘00’或‘01’
Lc	数据字节数
Data	报文鉴别代码（MAC）数据元；
Le	不存在

P2＝‘00’ ：此命令执行成功后可锁定应用，但该应用可以用 APPLICATION UNBLOCK 命令解锁。
P2＝‘01’：此命令执行成功后将永久锁定应用。

5.1.3 命令报文数据域

命令报文数据域包括报文鉴别码（MAC）数据元。

5.1.4 响应报文数据域

响应报文数据域不存在。

5.1.5 响应报文状态码

无论应用是否已经失效，此命令执行成功的状态码是‘9000’。
IC 卡可能回送的警告状态码如表 3-25 所示：
表 3-25　　APPLICATION BLOCK 警告状态

SW1	SW2	含　义

‘62’	‘00’	无信息提供
‘62’	‘81’	回送数据可能出错
‘62’	‘83’	选择文件无效

IC 卡可能回送的错误状态码如表 3-26 所示：

表 3-26　　APPLICATION BLOCK 错误状态

SW1	SW2	含　义
‘64’	‘00’	状态标志位未变
‘65’	‘81’	内存失败
‘69’	‘82’	不满足安全状态
‘69’	‘84’	引用数据无效
‘69’	‘87’	安全报文数据项丢失
‘69’	‘88’	安全报文数据项不正确
‘6A’	‘86’	参数 P1 P2 不正确
‘6A’	‘88’	未找到引用数据

5.2　APPLICATION UNBLOCK 命令

5.2.1　定义和范围

APPLICATION UNBLOCK 命令用于恢复当前应用。

当 APPLICATION UNBLOCK 命令成功地完成后，由 APPLICATION BLOCK 命令产生的对应用命令响应的限制将被取消。

5.2.2　命令报文

APPLICATION UNBLOCK 命令报文编码见表 3-27：

表 3-27　　APPLICATION UNBLOCK 命令报文

代码	值
CLA	‘84’
INS	‘18’
P1	‘00’，其他值保留为将来使用
P2	‘00’，其他值保留为将来使用
Lc	数据字节数
Data	报文鉴别代码（MAC）数据元；根据本标准第 8 篇中的规定进行编码
Le	不存在

5.2.3　命令报文数据域

命令报文数据域的内容包括报文鉴别代码（MAC）数据元。

5.2.4 响应报文数据域

响应报文数据域不存在。

5.2.5 响应报文状态码

不论应用是否已经失效，此命令执行成功的状态码是‘9000’。
IC 卡可能回送的错误状态码如表 3-28：
表 3-28　　APPLICATION UNBLOCK 错误状态

SW1	SW2	含　义
‘64’	‘00’	状态标志位未变
‘65’	‘81’	内存失败
‘69’	‘82’	不满足安全状态
‘69’	‘87’	安全报文数据项丢失
‘69’	‘88’	安全报文数据项不正确
‘93’	‘03’	应用已被永久锁定

5.3 CARD BLOCK 命令

5.3.1 定义和范围

CARD BLOCK 命令使卡中所有应用永久失效。
当 CARD BLOCK 命令成功地完成后，所有后续的命令都将回送状态码“不支持此功能”（SW1 SW2 =‘6A81’），且不执行任何其他操作。

5.3.2 命令报文

CARD BLOCK 命令报文编码见表 3-29：
表 3-29　　CARD BLOCK 命令报文

代码	值
CLA	‘84’
INS	‘16’
P1	‘00’，其他值保留为将来使用
P2	‘00’，其他值保留为将来使用
Lc	数据字节数
Data	报文鉴别代码（MAC）数据元；根据本标准第 8 篇中的规定进行编码
Le	不存在

5.3.3 命令报文数据域

命令报文数据域包括报文鉴别代码（MAC）数据元

5.3.4 响应报文数据域

响应报文数据域不存在。

5.3.5 响应报文状态码

此命令执行成功的状态码是‘9000’
IC 卡可能回送的错误状态码如表 3-30 所示：
表 3-30　　CARD BLOCK 错误状态

SW1	SW2	含　义
‘64’	‘00’	状态标志位未变
‘65’	‘81’	内存失败
‘69’	‘87’	安全报文数据项丢失
‘69’	‘88’	安全报文数据项不正确

5.4 EXTERNAL AUTHENTICATION 命令

5.4.1 定义和范围

EXTERNAL AUTHENTICATION 命令要求 IC 卡中的应用验证密码。
IC 卡的响应包括命令处理状态的回送。

5.4.2 命令报文

EXTERNAL AUTHENTICATION 命令报文编码见表 3-31：
表 3-31　　EXTERNAL AUTHENTICATION 命令报文

代码	值
CLA	‘00’
INS	‘82’
P1	‘00’
P2	‘00’
Lc	8－16
Data	发卡方认证数据
Le	不存在

EXTERNAL AUTHENTICATION 命令使用的算法参考值（P1）编码为‘00’表示无信息。算法参考值在命令发出之前是已知的，或者在数据域中提供。

5.4.3 命令报文数据域

命令报文数据域中包含 8~16 字节的数据：
——前 8 个必备型字节包含密码；
——可选的 1~8 个附加字节是专用的信息。

5.4.4 响应报文数据域

响应报文数据域不存在。

5.4.5 响应报文状态码

此命令执行成功的状态码是‘9000’
IC 卡可能回送的警告状态码如表 3-32 所示：
表 3-32　　EXTERNAL AUTHENTICATION 警告状态

SW1	SW2	含　义
‘63’	‘00’	认证失败

IC 卡可能回送的错误状态码如表 3-32 所示：

表 3-32　　EXTERNAL AUTHENTICATION 错误状态

SW1	SW2	含　义
‘67’	‘00’	Lc 不正确
‘69’	‘83’	认证方法锁定
‘6A’	‘86’	参数 P1 P2 不正确

5.5 GET CHALLENGE 命令

5.5.1 定义和范围

GET CHALLENGE 命令请求一个用于安全相关过程（例如：安全报文）的随机数。
除非掉电、选择了其他应用或又发出一个 GET CHALLENGE 命令，该随机数将一直有效。

5.5.2 命令报文

GET CHALLENGE 命令报文编码见表 3-33：
表 3-33　　GET CHALLENGE 命令报文

代码	值
CLA	‘00’
INS	‘84’
P1	‘00’
P2	‘00’
Lc	不存在
Data	不存在
Le	‘04’

5.5.3 命令报文数据域

命令报文数据域不存在。

5.5.4 响应报文数据域

响应报文数据域包括随机数，长度为 4 字节。

5.5.5 响应报文状态码

此命令执行成功的状态码是‘9000’。
IC 卡可能回送的错误状态码如表 3-34 所示：

表 3-34　　GET CHALLENGE 错误状态

SW1	SW2	含　义
‘6A’	‘81’	不支持此功能
‘6A’	‘86’	参数 P1 P2 不正确

5.6 GET RESPONSE 命令

5.6.1 定义和范围

当 APDU 不能用现有协议传输时，GET RESPONSE 命令提供了一种从卡片向接口设备传送 APDU（或 APDU 的一部分）的传输方法。

5.6.2 命令报文

GET RESPONSE 命令报文编码见表 3-35：

表 3-35　　GET RESPONSE 命令报文

代码	值
CLA	‘00’
INS	‘C0’
P1	‘00’
P2	‘00’
Lc	不存在
Data	不存在
Le	响应的期望数据最大长度

5.6.3 命令报文数据域

命令报文数据域不存在。

5.6.4 响应报文数据域

响应报文数据域的长度由 Le 的值决定。
如果 Le 的值为零，在附加数据有效时，卡片必须回送状态码‘6CXX’，否则回送状态码‘6F00’。

5.6.5 响应报文状态码

此命令执行成功的状态码是‘9000’。
表 3-36 列出正常处理情况：
表 3-36　　GET RESPONSE 正常状态

SW1	SW2	含　义
‘61’	‘XX’	正常处理，‘XX’表示可以通过后续 GET RESPONSE 命令得到的额外数据长度

IC 卡可能回送的警告状态码如表 3-37 所示：
表 3-37　　GET RESPONSE 警告状态

SW1	SW2	含　义
‘62’	‘81’	回送的数据可能有错

IC 卡可能回送的错误状态码如表 3-38 所示：
表 3-38　　GET RESPONSE 错误状态

SW1	SW2	含　义
‘67’	‘00’	长度错误（Le 不正确）
‘6A’	‘86’	参数 P1 P2 不正确
‘6C’	‘XX’	长度错误（Le 不正确，‘XX’表示实际长度）
‘6F’	‘00’	数据无效

5.7 INTERNAL AUTHENTICATION 命令

5.7.1 定义和范围

INTERNAL AUTHENTICATION 命令提供了利用接口设备发来的随机数和自身存储的相关密钥进行数据认证的功能。

5.7.2 命令报文

INTERNAL AUTHENTICATION 命令报文编码见表 3-39：
表 3-39　　INTERNAL AUTHENTICATION 命令报文

代码	值
CLA	‘00’
INS	‘88’
P1	‘00’

P2	‘00’
Lc	认证数据的长度
Data	认证数据
Le	‘00’

INTERNAL AUTHENTICATION 命令的参数 P1 为‘00’时的含义是无信息。P1 的值可事先得到，也可以在数据域中提供。
INTERNAL AUTHENTICATION 命令的参数 P2 为‘00’时的含义是无信息。P2 的值可事先得到，也可以在数据域中提供。

5.7.3 命令报文数据域

命令报文数据域的内容是应用专用的认证数据。

5.7.4 响应报文数据域

响应报文数据域内容是相关认证数据，其格式和定义见本标准第 2 部分。

5.7.5 响应报文状态码

此命令执行成功的码是‘9000’。
IC 卡可能回送的警告状态码如表 3-40 所示：
表 3-40　　INTERNAL AUTHENTICATION 警告状态

SW1	SW2	含　义
‘62’	‘81’	回送的数据可能有错

IC 卡可能回送的错误状态码如表 3-41 所示：
表 3-41　　INTERNAL AUTHENTICATION 错误状态

SW1	SW2	含　义
‘64’	‘00’	标志状态位未变
‘67’	‘00’	Lc 域不存在
‘68’	‘82’	不支持安全报文
‘69’	‘85’	不满足使用条件
‘6A’	‘80’	数据域参数不正确
‘6A’	‘86’	参数 P1 P2 不正确

5.8 PIN CHANGE／UNBLOCK 命令

5.8.1 定义和范围

PIN CHANGE／UNBLOCK 命令为发卡方提供了解锁个人密码，或者更改个人密码的功能。
当 PIN CHANGE／UNBLOCK 命令成功完成后，卡将执行以下功能：
——重置个人密码尝试计数器的值；

——产生新的个人密码（如果需要）。

命令中个人密码的传递采用加密方式。

5.8.2 命令报文

PIN CHANGE／UNBLOCK 命令报文编码见表 3-42：

表 3-42　　PIN CHANGE／UNBLOCK 命令报文

代码	值
CLA	‘84’；根据本标准第 8 篇中的规定进行编码
INS	‘24’
P1	‘00’
P2	‘00’或’01’
Lc	数据字节数
Data	加密的个人密码数据元和报文鉴别代码（MAC）数据元,根据本标准第 8 篇中的规定进行编码
Le	不存在

P2＝‘00’，表示解锁个人密码。此时应重置尝试计数器，但不更改个人密码。

P2＝‘01’，表示更改个人密码。此时应重置尝试计数器，并以一个新的个人密码取代原有个人密码。

当 P2＝‘00’时，Lc 应包括 MAC 数据元的长度。

当 P2＝‘01’时，Lc 应同时包括个人密码数据元和 MAC 数据元的长度。

5.8.3 命令报文数据域

命令报文数据域由个人密码数据元（如果存在）和其后的 MAC 数据元组成。

5.8.4 响应报文数据域

响应报文数据域不存在。

5.8.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

IC 卡可能回送的警告状态码如表 3-43 所示：

表 3-43　　PIN CHANGE／UNBLOCK 警告状态

SW1	SW2	含　义
‘62’	‘00’	无信息提供
‘62’	‘81’	数据可能出错

IC 卡可能回送的错误状态码如表 3-44 所示：

表 3-44　　PIN CHANGE／UNBLOCK 错误状态

SW1	SW2	含　义
‘64’	‘00’	状态标志位未变
‘65’	‘81’	内存失败

‘69’	‘82’	不满足安全状态
‘69’	‘84’	引用数据无效
‘69’	‘87’	安全报文数据项丢失
‘69’	‘88’	安全报文数据项不正确
‘6A’	‘86’	参数 P1 P2 不正确
‘6A’	‘88’	未找到引用数据
‘93’	‘03’	应用已被永久锁定

5.9　READ BINARY 命令

5.9.1　定义和范围

READ BINARY 命令用于读取二进制文件的内容（或部分内容）。

5.9.2　命令报文

READ BINARY 命令报文编码见表 3-45：

表 3-45　　READ BINARY 命令报文

代码	值
CLA	‘00’或‘04’
INS	‘B0’
P1	见表 3-46
P2	从文件中读取的第一个字节的偏移地址
Lc	不存在；（CLA＝‘04’时除外）
Data	不存在；（CLA＝‘04’时，应包括 MAC）
Le	‘00’

表 3-46 定义了命令报文中的引用控制参数：

表 3-46　　READ BINARY 命令引用控制参数

B8	b7	b6	b5	b4	b3	b2	b1	含　义
X 1								读取模式： －用 SFI 方式
	0	0						RFU（如果 b8＝1）
			X	X	X	X	X	SFI（取值范围 21－30）

5.9.3　命令报文数据域

一般情况下，命令报文数据域不存在。当使用安全报文时，命令报文数据域中应包含 MAC。MAC 的计算方法和长度由应用决定。

5.9.4 响应报文数据域

当 Le 的值为零时，只要文件的最大长度在 256（短长度）或 65535（扩展长度）之内，则其全部字节将被读出。

5.9.5 响应报文状态码

此命令执行成功的状态码是‘9000’。
IC 卡可能回送的警告状态码如表 3-47 所示：
表 3-47　　READ BINARY 警告状态

SW1	SW2	含　义
‘62’	‘81’	部分回送的数据可能有错
‘62’	‘82’	文件长度＜Le

IC 卡可能回送的错误状态码如表 3-48 所示：
表 3-48　　READ BINARY 错误状态

SW1	SW2	含　义
‘67’	‘00’	长度错误（Lc 域为空）
‘69’	‘81’	命令与文件结构不相容
‘69’	‘82’	不满足安全状态
‘69’	‘86’	不满足命令执行的条件（非当前 EF）
‘6A’	‘81’	不支持此功能
‘6A’	‘82’	未找到文件
‘6B’	‘00’	参数错误（偏移地址超出了 EF）
‘6C’	‘XX’	长度错误（Le 错误；‘XX’为实际长度）

5.10 READ RECORD 命令

5.10.1 定义和范围

READ RECORD 命令用于读取记录文件的内容。
IC 卡的响应由回送记录组成。

5.10.2 命令报文

READ RECORD 命令报文编码见表 3-49：
表 3-49　　READ RECORD 命令报文

代码	值
CLA	‘00’或‘04’
INS	‘B2’
P1	记录的序列号
P2	引用控制参数（见表 3-50）

Lc	不存在；（CLA＝‘04’时除外）
Data	不存在；（CLA＝‘04’时除外）
Le	‘00’

表 3-50 定义了命令报文中的引用控制参数：

表 3-50　　READ RECORD 命令引用控制参数

b8	b7	b6	b5	B4	b3	b2	b1	含　义
X	X	X	X	X				SFI
					1	0	0	P1 为记录的序列号

5.10.3 命令报文数据域

当无安全报文使用时，命令报文数据域不存在。使用安全报文时，命令报文的数据域中应包含 MAC。MAC 的计算方法和长度由应用决定。

5.10.4 响应报文数据域

所有执行成功的 READ RECORD 命令的响应报文数据域由读取的记录组成。

5.10.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

IC 卡可能回送的警告状态码如表 3-51 所示：

表 3-51　　READ RECORD 警告状态

SW1	SW2	含　义
‘62’	‘81’	回送的数据可能有错

IC 卡可能回送的错误状态码如表 3-52 所示：

表 3-52　　READ RECORD 错误状态

SW1	SW2	含　义
‘64’	‘00’	标志状态位没变
‘67’	‘00’	长度错误（Lc 域不存在）
‘69’	‘81’	命令与文件结构不相容
‘6A’	‘81’	不支持此功能
‘6A’	‘82’	未找到文件
‘6A’	‘83’	未找到记录

5.11 SELECT 命令

5.11.1 定义和范围

SELECT 命令通过文件名或 AID 来选择 IC 卡中的 PSE、DDF 或 ADF。应用选择在本标准的第 7 篇中

描述。
命令执行成功后，PSE、DDF 或 ADF 的路径被设定。
应用到 AEF 的后续命令将采用 SFI 方式联系到所选定的 PSE、DDF 或 ADF。
从 IC 卡的响应报文应由回送 FCI 组成。

5.11.2 命令报文

SELECT 命令报文编码见表 3-53：
表 3-53　　SELECT 命令报文

代码	值
CLA	‘00’
INS	‘A4’
P1	引用控制参数（见表 3-54）
P2	‘00’第一个或仅有一个 ‘02’下一个
Lc	‘05’－ ‘10’
Data	文件名
Le	‘00’

表 3-54 定义了命令报文中的引用控制参数：
表 3-54　　SELECT 命令引用控制参数

b8	b7	b6	b5	b4	b3	b2	b1	含　义
0	0	0	0	0				
					1			通过文件名选择
						0	0	

5.11.3 命令报文数据域

命令报文数据应包括所选择的 PSE 名、DF 名或 AID。

5.11.4 响应报文数据域

响应报文中数据域应包括所选择的 PSE、DDF 或 ADF 的 FCI。表 3-55 到表 3-57 规定了此定义所用的标志。本标准不规定 FCI 中回送的附加标志。
表 3-55 定义了成功选择 PSE 后回送的 FCI：
表 3-55　　SELECT PSE 的响应报文（FCI）

标志	值	存在方式
‘6F’	FCI 模板	M
‘84’	DF 名	M
‘A5’	FCI 专用数据	M
‘88’	目录基本文件的 SFI	M

表 3-56 定义了成功选择 DDF 后回送的 FCI：

表 3-56　　SELECT DDF 的响应报文（FCI）

标志	值	存在方式
‘6F’	FCI 模板	M
‘84’	DF 名	M
‘A5’	FCI 专用数据	M
‘88’	目录基本文件的 SFI	M

表 3-57 定义了成功选择 ADF 后回送的 FCI：

表 3-5 7　　SELECT ADF 的响应报文（FCI）

标志	值	存在方式
‘6F’	FCI 模板	M
‘84’	DF 名	M
‘A5’	FCI 专用数据	M
‘9F0C’	发卡方自定数据的 FCI	O

5.11.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

IC 卡可能回送的警告状态码如表 3-58 所示：

表 3-58　　SELECT 警告状态

SW1	SW2	含　义
‘62’	‘83’	选择的文件无效
‘62’	‘84’	FCI 格式与 P2 指定的不符

IC 卡可能回送的错误状态码如表 3-59 所示：

表 3-59　　SELECT 错误状态

SW1	SW2	含　义
‘64’	‘00’	标志状态位没变
‘67’	‘00’	P1 P2 与 Lc 不一致
‘6A’	‘81’	不支持此功能
‘6A’	‘82’	未找到文件
‘6A’	‘86’	参数 P1 P2 不正确

注：SW1 SW2＝‘6A82’用于表示当卡支持部分文件名选择时，没有与此部分文件名相匹配的文件。

5.12　UPDATE BINARY 命令

5.12.1 定义和范围

UPDATE BINARY 命令报文使用命令 APDU 中给定的数据修改 EF 文件中已有的数据。

5.12.2 命令报文

UPDATE BINARY 命令报文编码见表 3-60：

表 3-60　　UPDATE BINARY 命令报文

代码	值
CLA	‘00’
INS	‘D6’
P1	见表 3-61
P2	要修改的第一个字节的偏移地址
Lc	后续数据域的长度
Data	修改用的数据
Le	不存在

表 3-61 定义了命令报文中的引用控制参数：

表 3-61　　UPDATE BINARY 命令引用控制参数

b8	b7	b6	b5	b4	b3	b2	b1	含　义
X 1								读取模式： －用 SFI 方式
	0	0						RFU（如果 b8＝1）
			X	X	X	X	X	SFI（取值范围 21－30）

5.12.3 命令报文数据域

命令报文数据域包括更新原有数据的新数据。

5.12.4 响应报文数据域

响应报文数据域不存在。

5.12.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

IC 卡可能回送的警告状态码如表 3-62 所示：

表 3-62　　UPDATE BINARY 警告状态

SW1	SW2	含　义
‘63’	‘CX’	使用内部重试程序更新成功 X＝‘0’表示不提供计数器 X≠‘0’表示重试次数

IC 卡可能回送的错误状态码如表 3-63 所示：

表 3-63　　UPDATE BINARY 错误状态

SW1	SW2	含　义
‘65’	‘81’	内存失败（修改失败）

‘67’	‘00’	长度错误（Lc 域为空）
‘69’	‘81’	命令与文件结构不相容
‘69’	‘82’	不满足安全状态
‘69’	‘86’	不满足命令执行的条件（不是当前的 EF）
‘6A’	‘81’	不支持此功能
‘6A’	‘82’	未找到文件
‘6B’	‘00’	参数错误（偏移地址超出了 EF）

5.13　UPDATE RECORD 命令

5.13.1　定义和范围

UPDATE RECORD 命令报文用命令 APDU 中给定的数据更改指定的记录。

在使用当前记录地址时，该命令将在修改记录成功后重新设定记录指针。

5.13.2　命令报文

UPDATE RECORD 命令报文编码见表 3-64：

表 3-64　　UPDATE RECORD 命令报文

代码	值
CLA	‘00’
INS	‘DC’
P1	P1＝‘00’表示当前记录 P1≠‘00’指定的记录号
P2	见表 73
Lc	后续数据域的长度
Data	更新原有记录的新记录
Le	不存在

表 3-65 定义了命令报文中的引用控制参数：

表 3-65　　UPDATE RECORD 命令引用控制参数

b8	b7	b6	b5	b4	b3	b2	b1	含　义
X	X	X	X	X				SFI
					0	0	0	第一个记录
					0	0	1	最后一个记录
					0	1	0	下一个记录
					0	1	1	上一个记录
					1	0	0	记录号在 P1 中给出
其余值								RFU

5.13.3 命令报文数据域

命令报文数据域由更新原有记录的新记录组成。

5.13.4 响应报文数据域

响应报文数据域不存在。

5.13.5 响应报文状态码

此命令执行成功的状态码是‘9000’。
IC 卡可能回送的警告状态码如表 3-66 所示：
表 3-66　　UPDATE RECORD 警告状态

SW1	SW2	含　义
‘63’	‘CX’	使用内部重试程序更新成功 X＝‘0’表示不提供计数器 X≠‘0’表示重试次数

IC 卡可能回送的错误状态码如表 3-67 所示：
表 3-67　　UPDATE RECORD 错误状态

SW1	SW2	含　义
‘65’	‘81’	内存失败（修改失败）
‘67’	‘00’	长度错误（Lc 域为空）
‘69’	‘81’	命令与文件结构不相容
‘69’	‘82’	不满足安全状态
‘69’	‘86’	不满足命令执行的条件（不是当前的 EF）
‘6A’	‘81’	不支持此功能
‘6A’	‘82’	未找到文件
‘6A’	‘83’	未找到记录
‘6A’	‘84’	文件中存储空间不够

5.14　VERIFY 命令

5.14.1 定义和范围

VERIFY 命令用于校验命令数据域中的个人密码的正确性。

5.14.2 命令报文

VERIFY 命令报文编码见表 3-68：
表 3-68　　VERIFY 命令报文

代码	值
CLA	‘00’

INS	‘20’
P1	‘00’
P2	‘00’
Lc	可变
Data	外部输入的个人密码
Le	不存在

P2＝‘00’表示无特殊限定符被使用。在 IC 卡上，VERIFY 命令在处理过程中应明确知道如何去寻找个人密码。

5.14.3 命令报文数据域

命令报文域由持卡者输入的个人密码组成。

5.14.4 响应报文数据域

响应报文数据域不存在。

5.14.5 响应报文状态码

此命令执行成功的状态码是‘9000’。
当前的应用选择中，命令数据域中外部输入的个人密码与卡中存放的个人密码校验失败时，IC 卡将回送 SW2＝‘Cx’， ‘x’表示个人密码允许重试的次数；当卡回送‘C0’时，表示不能重试个人密码。此时再使用 VERIFY 命令时，将回送失败状态码 SW1 SW2＝‘6983’。
IC 卡可能回送的警告状态码如表 3-69 所示：

表 3-69　　VERIFY 警告状态

SW1	SW2	含　义
‘63’	‘Cx’	校验失败，‘x’表示允许重试的次数

IC 卡可能回送的错误状态码如表 3-70 所示：

表 3-70　　VERIFY 错误状态

SW1	SW2	含　义
‘64’	‘00’	标志状态位没变
‘69’	‘83’	认证方法（个人密码）锁定
‘69’	‘84’	引用数据无效
‘6A’	‘86’	参数 P1 P2 不正确
‘6A’	‘88’	未找到引用数据

5.15　CHANGE　PIN 命令

5.15.1 定义和范围

CHANGE PIN 允许持卡人将当前个人密码修改为新的密码。

当 CHANGE PIN 命令成功完成后，卡片要进行以下操作：

——密码尝试计数器复位至密码尝试次数的上限；

——将原个人密码置为新的个人密码。

此命令中的个人密码（PIN）值以明文方式传送。命令数据中个人密码（PIN）是以'cn'格式存放的，它不需要整字节的填充，只有最低有效字节的低半字节可能需要填充，且填以'F'。

5.15.2 命令报文

CHANGE PIN 命令报文见表 3-71：

表 3-71　　CHANGE PIN 命令报文

代码	值
CLA	'80'
INS	'5E'
P1	'01'
P2	'00'
L_c	'05'－ '0D'
Data	当前 PIN||'FF'||新的 PIN
L_e	不用

5.15.3 响应报文数据域

响应报文的数据域不存在。

5.15.4 响应报文的状态码

此命令执行成功的状态码是'9000'。

表 3-72 描述了 IC 卡可能回送的错误状态码：

表 3-72　　CHANGE PIN 错误状态

SW1	SW2	含　义
'63'	'Cx'	验证失败，还剩下 X 次尝试机会
'65'	'81'	内存错误
'69'	'83'	验证方法锁定
'69'	'85'	使用条件不满足
'6A'	'80'	数据域参数不正确
'6A'	'86'	P1、P2 参数不正确

5.16　RELOAD PIN 命令

5.16.1　定义和范围

RELOAD PIN 命令用于发卡方重新给持卡人产生一个新的 PIN（可以与原 PIN 相同）。

RELOAD PIN 只能在拥有或能访问到重装 PIN 子密钥（DRPK）的发卡方终端（例如发卡方银行终端）上执行。

在成功执行 RELOAD PIN 命令后，IC 卡必须完成以下操作：

——PIN 错误尝试计数器复位。

——IC 卡的原 PIN 必须设置为新的 PIN 值。

命令中的 PIN 数据以明文传送。

5.16.2　命令报文

RELOAD PIN 命令报文见表 3-73：

表 3-73　　RELOAD PIN 命令报文

代码	值
CLA	‘80’
INS	‘5E’
P1	‘00’
P2	‘00’
L_c	‘06’~’OA’
Data	见表 3-74
L_e	不存在

5.16.3　命令报文数据域

表 3-74　　RELOAD PIN 命令报文数据域

说明	长度（字节）
重装的 PIN 值	2－6
MAC	4

用 DRPK 左右 8 位字节进行异或运算作的结果按照附录 B 中描述的机制对新 PIN 值计算 MAC。

5.16.4　响应报文数据域

响应报文的数据域不存在。

5.16.5 响应报文的状态码

此命令执行成功的状态码是'9000'。

表 3-75 描述了 IC 卡可能回送的错误状态码：

表 3-75　　RELOAD PIN 错误状态

SW1	SW2	说　　明
'65'	'81'	内存错误
'67'	'00'	长度错误
'69'	'85'	使用条件不满足
'69'	'88'	安全信息数据对象不正确
SW1	SW2	含义
'6A'	'86'	P1、P2 参数不正确
'6A'	'88'	引用数据找不到
'93'	'03'	应用永久锁住

5.17　专用 DES 计算

5.17.1 定义和范围

DES 和命令利用指定的密钥来进行运算。若一条命令无法传输所有的待处理数据，可分几条命令输入。

加密计算采用 ECB 模式，数据的填充在卡片外面进行，卡片只支持长度为 8 的整数倍数据的加密。

命令的执行前必须先验证卡片的 PIN。

5.17.2 命令报文

DES CRYPT 命令报文见表 3－76。

表 3－76　DES CRYPT 命令报文

代码	值
CLA	80h
INS	A8h
P1	00
P2	密钥索引
Lc	08h　　要加密的数据长度
Data	要加密的数据
Le	不存在

5.17.3 命令报文数据域

命令报文数据域包括要加密的数据（8 字节长度）。

5.17.4 响应报文数据域

响应报文数据域包括加密结果，数据长度是 8 字节。

5.17.5 响应报文的状态码

执行成功返回 9000。表 3－77 为错误状态码。

表 3－77　DES CRYPT 命令状态码

SW1	SW2	含义
64	00	标志状态位没变
65	81	内存失败
67	00	长度错误
69	01	命令不接受（无效状态）
69	85	使用条件不满足（应用被锁定）
69	86	不满足命令执行条件，当前文件不是 EF
6A	81	应用锁定
6A	86	P1 或 P2 不正确
6D	00	INS 不正确
6E	00	CLA 不正确
93	03	应用被永久锁定

6　PSAM 卡数据结构

PSE 的 AID：1PAY.SYS.DDF01

中石化应用 1 AID = A0 00 00 00 03 “SINOPEC1”

中石化应用 2 AID = A0 00 00 00 03 “SINOPEC2”

6.1　卡片公共信息文件

文件标识（SFI）		‘21’（十进制）
文件类型		透明
文件大小		14
文件存取控制	读＝自由	改写＝需要安全信息

字节	数据元	长度/默认值
1－10	PSAM 序列号	10/见应用序列号定义
11	PSAM 版本号=00	1/00
12	密钥卡类型=01	1/01
13	指令集版本=01	1/01
14	发卡方自定义 FCI 数据=00	1/00

6.2　终端信息文件

文件标识（SFI）		‘22’（十进制）
文件类型		透明
文件大小		6
文件存取控制	读＝自由	改写＝需要安全信息

字节	数据元	长度
1－6	终端机编号	6/见终端机号结构

6.3　终端机号结构

长度	内容	说明/默认值
1	行业	1=中石化加油(气)
2	终端类型	3=加油(气)机，参见中石化 IC 卡规范
3~4	地区号	按照中石化省编码
5~12	顺序号	顺序号/自定义

6.4　中国石化应用 1 的应用公共信息文件

文件标识（SFI）	‘23’（十进制）
文件类型	透明

文件大小			25
文件存取控制		读＝自由	改写＝需要安全信息
字节	数据元		长度/默认值
1	全国加油(气)消费密钥索引号=01（02）		1/01（02）
2－9	应用发行者标识		8/10FFFFFFFFFFFFF
10－17	应用接收者标识		8/35FFFFFFFFFFFFF
18－21	应用启用日期		4//20100901
22－25	应用有效日期		4/20121231

6.5　中国石化应用 1 的密钥文件

数据元		索引
加油(气)消费密钥	MPK1	01
专用密钥	ANTI_K	01
专用密钥	ACTK	01
专用密钥	RIDK	01
日志 MAC 计算密钥	MMACKEY	01

6.6　中国石化应用 2 的密钥文件

数据元		版本
SAMTAC	MSTACK	01
计算密钥	MMACKEY	01

7　　ACT 卡数据结构

PSE 的 AID：1PAY.SYS.DDF01

7.1　应用环境目录文件

文件标识（SFI）		‘01’（十进制）
文件类型		变长线性
文件大小		
文件存取控制	读=自由	改写＝需要安全信息
数据元		
石化应用	AID=A0 00 00 00 03 “SINOPEC”	

7.2　石化应用

文件存取控制	建立文件＝需要安全权限（卡商自定义，不能为自由）	
	应用锁定=需要安全信息	应用解锁=需要安全信息

7.3　石化应用的公共应用基本数据文件

文件标识（SFI）		‘21’（十进制）
文件类型		透明
文件大小		30
文件存取控制	读=自由	改写＝需要 安全信息
字节	数据元	长度/默认值
1～8	发卡方标识	8/35FFFFFFFFFFFFF
9	应用类型标识=0x11	1/11
10	应用版本=01	1/01
11～20	ACT 卡卡号	参见数据元说明部分
21～24	应用启用日期	4/20100830
25～28	应用有效日期	4/20151231
29	指令集版本	1/01
30	备用	1/00

7.4　石化应用的持卡人基本数据文件

文件标识（SFI）	‘26’（十进制）
文件类型	透明
文件大小	41

文件存取控制	读=自由	改写＝需要 安全信息
字节	数据元	长度/默认值
1	认证密钥索引号（ACT 索引号）	1/01
2	保留	1/00
3～22	持卡人姓名	20/11111111111111111111111111111111111111
23～40	持卡人证件号码	18/”123456789012345678X”(ASCII 码)
41	持卡人证件类型	1/01

7.5　ACT 卡管理密钥

数据元	默认值
卡片主控密钥	
应用主控密钥	
卡片维护密钥	MFMAMK
应用维护密钥	MAMK
密码解锁密钥	MPUK
密码重装密钥	MRPK
计算密钥	MMACKEY

7.6　个人密码（PIN）

数据元	默认值（BCD）
PIN	9999

8　　RID 卡数据结构

PSE 的 AID：1PAY.SYS.DDF01

8.1　应用环境目录文件

文件标识（SFI）		‘01’（十进制）
文件类型		变长线性
文件大小		
文件存取控制	读=自由	改写＝需要安全信息
数据元		
石化应用	AID=A0 00 00 00 03 “SINOPEC”	

8.2　石化应用

文件存取控制	建立文件＝需要安全权限（卡商自定义，不能为自由）	
	应用锁定=需要安全信息	应用解锁=需要安全信息

8.3　石化应用的公共应用基本数据文件

文件标识（SFI）		‘21’（十进制）
文件类型		透明
文件大小		30
文件存取控制	读=自由	改写＝需要安全信息
字节	数据元	长度/默认值
1～8	油机厂商标识	8/3031FFFFFFFFFFF
9	应用类型标识=0x11	1/11
10	应用版本=01	1/01
11～20	RID 卡卡号	参见数据元说明部分
21～24	应用启用日期	4/20100830
25～28	应用有效日期	4/20151231
29	指令集版本	1/01
30	备用	1/00

8.4　石化应用的持卡人基本数据文件

文件标识（SFI）		‘26’（十进制）
文件类型		透明
文件大小		41
文件存取控制	读=自由	改写＝需要安全信息
字节	数据元	长度/默认值

1	认证密钥索引号（RID 索引号）	1/01
2	计算密钥版本号（日志 MAC 计算）	1/01
3～22	持卡人姓名	20/11111111111111111111111111111111
23～40	持卡人证件号码	18/”123456789012345678X”(ASCII 码)
41	持卡人证件类型	1/01

8.5　石化应用的内部记录文件

文件标识（SFI）		无
文件类型		内部文件
记录个数		150
文件存取控制	读=自由	改写＝需要 PIN
字节	数据元	长度/默认值
1～7	启动绑定日期时间	7/20101231010101
8～17	ACT 卡卡号	10/01005013500000000001
18	ACT 卡认证密钥索引	1/01
19～28	RID 卡卡号	10/01005110100000000001
29	RID 卡认证密钥索引	1/01
30	日志 MAC 计算密钥索引	1/01
31～40	PSAM 卡卡号	10/01001013500000000001
41～48	油机芯片 ID	8/3031534535355679
49～52	校验 MAC	23A4FF21

8.6　RID 卡管理密钥

数据元	默认值
卡片主控密钥	
应用主控密钥	
卡片维护密钥	MFMAMK
应用维护密钥	MAMK
密码解锁密钥	MPUK
密码重装密钥	MRPK
计算密钥	MMACKEY

8.7　个人密码（PIN）

数据元	默认值（BCD）
PIN	9999

9　数据元说明

9.1　卡应用序列号结构

顺序	内容	说明/默认值（BCD）
0	保留	填 0
1	行业	1=中石化
2~3	合作银行代号	00=无
4~5	卡类型	10=PSAM 卡、50=ACT 卡、51=RID 卡 其他值保留
6	批次	密钥版本/1
7~8	地区号/厂商编号（如果是 RID 卡则该字段及其后 2 位为油机厂家 ID）	地区号： 按照中石化省编码, （10=中石化） 11=北京、12=天津 13=河北、14=山西 31=上海、32=江苏 33=浙江、34=安徽 35=福建、36=江西 37=山东、41=河南 42=湖北、43=湖南 44=广东、45=广西 46=海南、52=贵州 53=云南、90=深圳 51-川渝 油机厂家ID： 3031-正星科技 3032-北京长吉 3033-稳恩佳力佳 3034-厦门榕兴 3035-北京三盈 3036-托肯恒山 3037-德莱赛稳 3038-上海中意 3039-江阴富仁
9~10	保留（如果是 RID 卡则该字段被占用为油机厂家 ID）	全部填0
11~19	顺序号	顺序号

9.2　加油机计量芯片 ID 结构(BCD 格式)

顺序	内容	说明/默认值
0~3	油机厂商 ID	油机厂商ID分配：① 3031-正星科技 3032-北京长吉 3033-稳恩佳力佳 3034-厦门榕兴 3035-北京三盈 3036-托肯恒山 3037-德莱赛稳 3038-上海中意 3039-江阴富仁
4~15	计量芯片生产序列号	厂家负责序号的唯一性

①说明：0000102030405060 用于测试目的，0000 不分配给厂家。

9.3　加油机发送给管控的报错信息报文中 Data 域格式

（1） 说明：本节所述的“加油机发送给管控的报错信息报文中 Data 域”是指——*中国石化加油 IC 卡工程《加油站卡机联动电脑加油机与监控 PC 机通讯数据接口协议》(试行稿 V1.1) 中第十章“数据交换命令”之第 8 节“加油机向 PC 机发送加油机内部出错信息”功能* 所涉及的 Data 域。

（2） Data 域组成及格式如下表：

加油机报错信息报文中 Data 域的格式（92 个可显示 ASCII 字符，每个字符占 1 个字节）									
报文分类 8 chars	厂商编号 2 chars	软件版本 4 chars	日期时间 14 chars	计量芯片 ID 16 chars	厂商自定① 16 chars	PSAM 卡号 20 chars	验算 MAC 8 chars	校验 CRC 4 chars	备注
#*0011*#	01	1012	20110428153758	3031990123456789	38D3CDBBFA000000	01001013700123456789	251798A2	C366	注册启用信息
#*1122*#									安全报警信息
#*2233*#									报警信息/同类错误仅报 1 次
其他值									老油机错误信息

注释：① 前 2 字符为数字型,用于标识计量芯片认证剩余次数，如 06 次、38 次、50 次等，其余 14 字符厂商自定(默认值填 0)。
上表中“ #*0011*# ”行中各域所填数据是示例目的，使用时请根据实际情况填写。

（3） 有关 MAC 和 CRC 计算的说明

(a)验算 MAC 的计算：

参与计算的数据及格式如下：

数据项	长度（字节）	格式	示例
厂商编号	1	Bcd	‘01’表示 3031
软件版本	2	Bcd	‘10’ ’ 12’表示V1.0.1.2
日期时间	7	Bcd	‘20’ ’ 11’ ’ 04’ ’ 28’ ’ 15’ ’ 37’ ’ 58’
芯片 ID	8	Bcd	‘30’ ’ 31’ ’ 99’ ’ 01’ ’ 23’ ’ 45’ ’ 67’ ’ 89’
厂商自定	8	Hex	‘38’ ’ D3’ ’ CD’ ’ BB’ ’ FA’ ’ 00’ ’ 00’ ’ 00’/默认值填 ’ 00’
PSAM 卡号	10	Bcd	‘01’ ’ 00’ ’ 10’ ’ 13’ ’ 70’ ’ 01’ ’ 23’ ’ 45’ ’ 67’ ’ 89’

采用的算法及密钥：采用*中国石化加油 IC 卡工程《加油站卡机联动电脑加油机与监控 PC 机通讯数据接口协议》(试行稿 V1.1)*中*“关于 MAC 的计算”*所述的算法和密钥。

计算步骤示例：

第一步：以8 字节‘00 00 00 00 00 00 00 00’作为初始值。

第二步：计算范围从厂商编号到PSAM 卡号的连接在一起形成的数据体。

第三步：将该数据体分成8字节为单位的数据块，标号为D1，D2，D3，D4等，最后的数据块有可能是1-8个字节。

第四步：如果最后的数据块长度是8字节的话，则在其后加上16进制数字‘80 00 00 00 00 00 00 00’，转到第五步。如果最后的数据块长度不足8字节的话，则在其后加上16进制数字‘80’，如果达到8字节长度，则转入第五步；否则在‘80’后再加入16进制数字‘00’直到长度达到8字节。

第五步：对这些数据块使用PSAM卡内的省通讯密钥计算MAC。
第六步：取计算结果的前4个字节作为验算MAC。将4字节MAC之每个字节拆分成2个、共8个可显示ASCII字符作为验算MAC报文。

示例：计算出的 4 个字节为 0x25 0x17 0x98 0xa2，拆分成 8 个字符：251798A2，作为验算 MAC 报文。

(b)校验 CRC 的计算：

参与计算的数据及格式如下：

数据项	长度（字节）	格式	示例
厂商编号	1	Bcd	‘01’表示　3031
软件版本	2	Bcd	‘10’ ’12’表示V1.0.1.2
日期时间	7	Bcd	‘20’ ’11’ ’04’ ’28’ ’15’ ’37’ ’58’
芯片 ID	8	Bcd	‘30’ ’31’ ’99’ ’01’ ’23’ ’45’ ’67’ ’89’
厂商自定	8	Hex	‘38’ ’D3’ ’CD’ ’BB’ ’FA’ ’00’ ’00’ ’00’
PSAM 卡号	10	Bcd	‘01’ ’00’ ’10’ ’13’ ’70’ ’01’ ’23’ ’45’ ’67’ ’89’
验算 MAC	4	Hex	‘25’ ‘17’ ‘98’ ‘A2’

采用的算法：采用*中国石化加油 IC 卡工程《加油站卡机联动电脑加油机与监控 PC 机通讯数据接口协议》(试行稿 V1.1)*中《附录 3：CRC 原理和算法》所述的算法，即 CRC 多项式为 0xA001、初始值为 0x0000。

将计算出的 2 个字节 CRC 值，如 0xC366，拆分成 4 个可显示 ASCII 字符 C366 作为校验 CRC 报文。

10　税控模组、计量部分安全功能提升

10.1　升级税控模组编码器

要求 2011 年 7 月 1 日后的新标准加油机使用功能升级后的防作弊税控模组和编码器。

10.2　完善静电释放流程及税控显示屏安全性能

无密码用户卡插卡加油时，键显屏提示“请按确认键”，用户须先按键盘的确认键再显示余额加油，以充分释放静电，验证 IC 卡密码后进行灰卡状态检查及解灰流程。

自助加油机挂枪后汉显键盘显示并语音播报加油金额和加油量；卡机联动加油机挂枪后汉显键盘显示加油金额和加油量，宜语音播报加油金额和加油量；显示内容保持 1 秒至 3 秒钟。

10.3　完善主显示重显功能

禁止通过加油机主显示屏重显加油数据，可通过键盘显示屏显示历史加油数据。

11　加油 IC 卡内剩余 0.1 升油量金额功能的修改

非定量加油时，加油机按卡内余额值以定额方式加油，可将加油卡内余额消费为 0 元，卡内不再剩余 0.1 升油的金额，加油机的控制按定量加油模式处理，若卡内余额小于 1 升，则不能开机加油。

若电磁阀或机器故障可能导致加油量过冲，此种情况加油机按实际加油量显示。挂枪后加油机先将卡内余额扣完后产生一笔正常的交易，再产生一笔非卡交易补足过冲的数额。加油机先不退卡并提示“加油量超过卡余额，过冲金额##元”。过冲加油金额由油站与用户协商解决后，按退卡键再输入员工密码后退卡。以上情况都不会造成锁卡，卡片可以重新充值使用。若加油机连续过冲 3 次或连续过冲值超过 5 升则加油机锁机并提示加油机故障。