ICS 35.240
L 65

中华人民共和国国家标准

GB/T 39465—2020

城市智慧卡互联互通　充值数据接口

Card of smart city union—Interface for charging data

2020-11-19 发布　　2021-06-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由中华人民共和国住房和城乡建设部提出。

本标准由全国智能建筑及居住区数字化标准化技术委员会(SAC/TC 426)归口。

本标准起草单位:北京亿速码数据处理有限责任公司、中外建设信息有限责任公司、城联数据有限公司、北京智芯微电子科技有限公司、东信和平科技股份有限公司、中城智物联网技术研究(深圳)有限公司、天津通卡智能网络科技股份有限公司、山东华冠智能卡有限公司、上海复旦微电子集团股份有限公司、浙江创建科技有限公司、北京握奇数据股份有限公司、武汉天喻信息产业股份有限公司、青岛海纳云科技控股有限公司、广东天波教育科技有限公司、广东永华通讯科技有限公司、杭州国朗科技有限公司、珠海市珠海通科技有限公司、中建新疆建工(集团)有限公司。

本标准主要起草人:蔡文成、张永刚、谢跃文、马虹、王莎、金学明、范琳琳、周亮、尚治宇、孙式方、李小帅、林翌桢、白婧、徐湖伟、李德昶、何全、梁浩炘、张佳燕、沈阳、李世强。

城市智慧卡互联互通　充值数据接口

1　范围

本标准规定了城市智慧卡互联互通充值架构及功能、报文和接口数据定义、充值申请、充值操作、充值异常处理及对账文件处理等。

本标准适用于城市智慧卡互联互通充值数据接口的设计、开发和应用。

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 1988—1998　信息技术　信息交换用七位编码字符集

GB/T 13000—2010　信息技术　通用多八位编码字符集(UCS)

GB/T 31778—2015　数字城市一卡通互联互通　通用技术要求

3　术语和定义

下列术语和定义适用于本文件。

3.1

城市智慧卡　card of smart city

用于城市内综合交通(公共汽车、地铁、轻轨、轮渡、出租车、公共自行车)、公共事业缴费、风景园林、社区/园区应用、停车场管理等多项业务需求，具有微处理器芯片的识别卡。

注：本标准中提到的IC卡均指城市智慧卡。

3.2

充值平台　platform for charge

通过通信网络实现对城市智慧卡充值申请、操作、异常处理和对账的系统。

3.3

清分　clearing

当日的全部网络交易数据按照平台间进行汇总、整理、分类的过程。

3.4

报文　message

充值终端和城市智慧卡相互发送，不含传输控制字符的字节串。

3.5

圈存　load

持卡人将相关账户上的资金划转到城市智慧卡电子钱包的过程。

[JR/T 0025.2—2010，定义 3.19]

4　缩略语

下列缩略语适用于本文件。

APDU　应用协议数据单元(Application Protocol Data Unit)

APP　应用(Application)
eSE　嵌入式安全单元(embedded Secure Element)
FTP　文件传输协议(File Transfer Protocol)
HCE　基于主机的卡模拟(Host-based Card Emulation)
IC　集成电路(Integrated Circuit)
ID　身份标识号(Identity)
JSON　脚本对象简谱(JavaScript Object Notation)
MAC　报文认证码(Message Authentication Code)
MD5　报文摘要算法 5(Message-Digest Algorithm　5)
RSA　非对称加密算法(Rivest/Shamir/Adleman asymmetric algorithm)
SE　安全单元(Secure Element)
SM2　安全消息算法 2(Secure Message 2)

5　充值架构及功能

5.1　系统充值架构

城市智慧卡互联互通平台与第三方充值平台的充值数据接口应按照充值申请、充值操作、充值异常处理、对账文件处理的流程进行规范,并约定报文和接口数据要求。城市智慧卡第三方充值架构,见图 1。

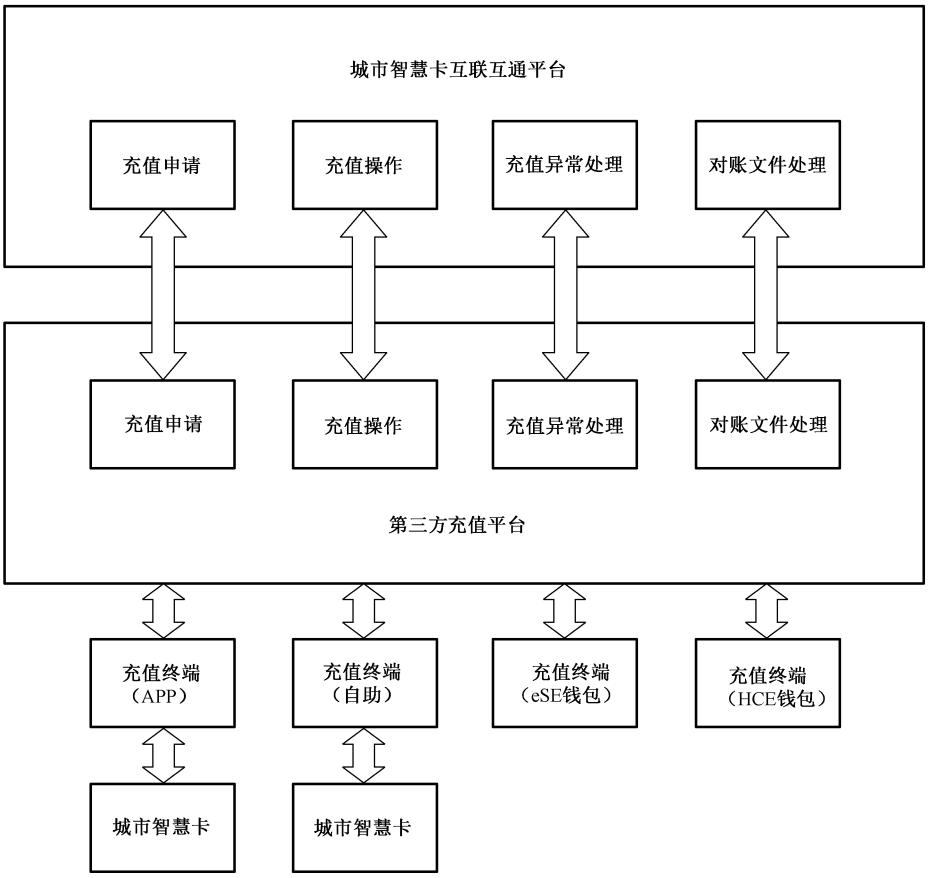

图 1　城市智慧卡第三方充值架构

5.2 功能要求

城市智慧卡互联互通平台充值数据接口应符合下列要求：

a) 应具备与第三方充值平台的充值申请、充值操作和充值异常处理、对账文件处理等进行对接的功能；

b) 应实现充值数据的清分结算和第三方充值平台对账文件的处理，清分结算内容应符合GB/T 31778—2015的规定；

c) 宜兼容手机APP充值终端、自助充值终端、手机eSE钱包和手机HCE钱包等多种充值方式。

6 报文和接口数据定义

6.1 报文格式说明

报文格式应符合下列要求：

a) 通信方式应采用请求-响应协议，使用投递方式提交请求参数，编码字符集应符合GB/T 1988—1998和GB/T 13000—2010中8位元(UTF-8)的要求。数据的格式应为JSON格式。

示例1：{"Version":"1.0","Format":"JSON","Charset":"UTF-8","Timestamp":"2019-03-28 11:30:45","Sign_type":"RSA","sign":"******","Parastr":"请求参数报文集合"}(注意：发送报文为：data={"Version":"1.0","Format":"JSON","Charset":"UTF-8","Timestamp":"2019-03-28 11:30:45",Sign_type":"RSA","Sign":"******","Parastr":"请求参数报文集合"})。

报文体内容也应为JSON格式。

示例2：{"Name":"charge","Plat_id":"2253123456781234","App_id":"123456790010",CardNo:"1234567890123456"}。

b) 应答参数数据格式应为JSON格式。

示例3：{"Version":"1.0","Format":"JSON","Charset":"UTF-8","Timestamp":"2019-03-28 11:30:45","Sign_type":"RSA","Sign":"******","Parastr":"返回参数集合"}。

报文体内容也应为JSON格式。

示例4：{"Name":"charge","Plat_id":"2253123456781234","App_id":"123456790010",CardNo:"1234567890123456"}。

c) 报文中的数据应区分大小写。

d) 通信应使用短链接。

6.2 报文安全说明

报文安全应符合下列要求：

a) 报文内容中应包含签名信息，报文发送方用本方的私钥对报文进行签名，报文接收方用对方的公钥验签，当服务端验签失败，应返回失败并丢弃报文；

b) 通卡平台应下发公钥给充值平台，充值平台接入通卡平台前，应提供公钥给通卡平台，通卡平台将充值平台的公钥进行配置。

6.3 接口及数据域定义

接口及数据域定义应符合表1的规定。

表 1　接口及数据域定义

序号	内容	名称	类型	备注
1	通用请求参数	Version	String	接口版本号
2		Format		请求参数格式，仅支持 JSON
3		Charset		应符合 GB/T 1988—1998 和 GB/T 13000—2010 中 UTF-8 的要求
4		Timestamp		发起请求的时间，yyyy-MM-dd HH:mm:ss 格式
5		Sign_type		签名方式，SM2、MD5、RSA 等
6		Sign		签名
7		Parastr		参数集合
8	充值交易参数	Name		交易类型名称，含验卡、圈存、查询
9		Plat_id		发起充值请求的平台标识
10		App_id		充值服务提供商在充值平台上的注册 ID
11		CardNo		卡号，卡密钥分散因子
12		Orderid		充值订单号、流水号
13		OrderStatus		充值订单状态，分订单创建、充值成功、充值失败、充值异常、订单关闭、订单处理中等用于标识订单在交易流程中的不同情况
14		Amount		充值金额
15		Pay_type		交易支付类型
16		APDUset		APDU 指令序列，可包含多个 APDU 指令
17		APDUresp		APDU 指令执行结果，可包含多个 APDU
18		APDUver		支持多版本 APDU，可用于标识 APDU 是否加密
19		APDUflag		0：APDU 指令信息为非空，下发 APDU 指令，执行完 APDU 指令后 提交结果继续圈存过程。 1：APDU 指令信息为空，圈存结束
20		TerminalNo		终端机编号
21		Statuscode		状态码，0：成功；非 0 为其他错误码
22		Statusdescription		状态描述

7　充值申请

7.1　操作流程

充值申请操作应符合下列要求：

a）　充值申请操作应包括订单预处理和订单确认；

b）　持卡人应通过充值终端连接充值平台，通过充值平台与通卡后台的充值申请接口通信，实现 IC 卡的充值申请操作，并完成向通卡平台账户的充值；

c）　充值申请时序图见图 2。

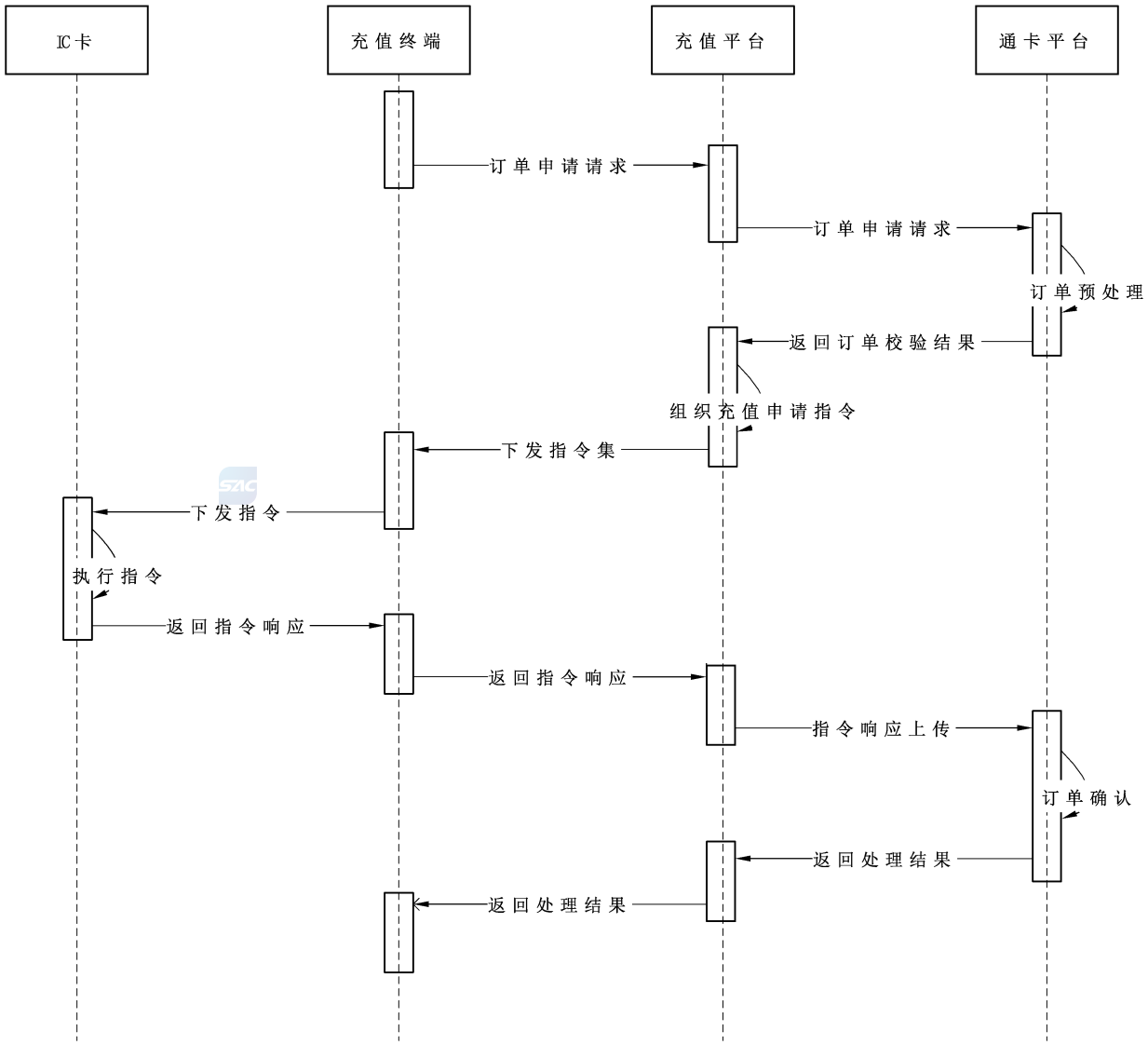

图 2　充值申请时序图

7.2　通卡平台充值申请流程

7.2.1　一般规定

通卡平台充值申请业务流程见图 3。

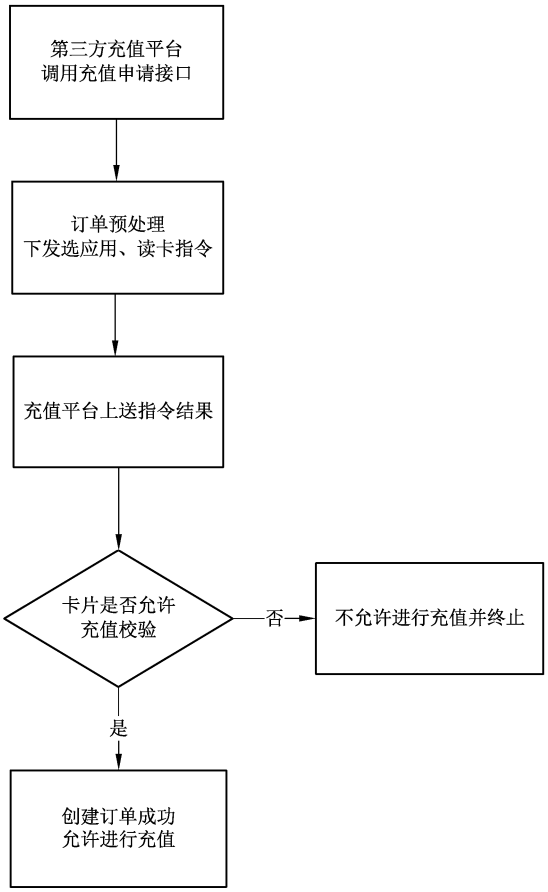

图 3　通卡平台充值申请业务流程

7.2.2　订单预处理

当充值平台接收到充值终端发起的充值申请时，应验证申请报文是否符合 6.3 的要求，同时将订单请求上送给通卡平台验证订单状态是否合法。当得到通卡平台的验证结果后，如果不合法，应申请终止，否则组织并下发读取 IC 卡指令，启动充值申请操作。

7.2.3　订单确认

充值终端接收并向 IC 卡转发指令，IC 卡执行相应指令，并将结果返回。充值终端收到命令响应报文后，通过充值平台将响应数据传给通卡后台。通卡平台确认该 IC 卡是否正常，从而做最终的订单确认。当订单确认成功，则进行接下来的充值操作；否则，需返回错误状态至充值平台，充值平台通知充值终端中止交易。

订单确认包含的内容如下：

a）　IC 卡读取指令返回码认证；
b）　IC 卡是否为本系统卡；
c）　IC 卡是否为黑名单；
d）　IC 卡状态是否正常（是否锁定或退卡）；
e）　充值余额是否达到上限。

8　充值操作

8.1　一般规定

持卡人通过充值终端连接充值平台，通过充值平台与通卡后台的充值接口通信，实现 IC 卡充值操作，持卡人可将相应账户上的资金划入电子存折或电子钱包中。充值操作接口应支持用户充值平台和

通卡后台间信息交互，交易过程可能存在多次交互。

充值操作流程见图 4。

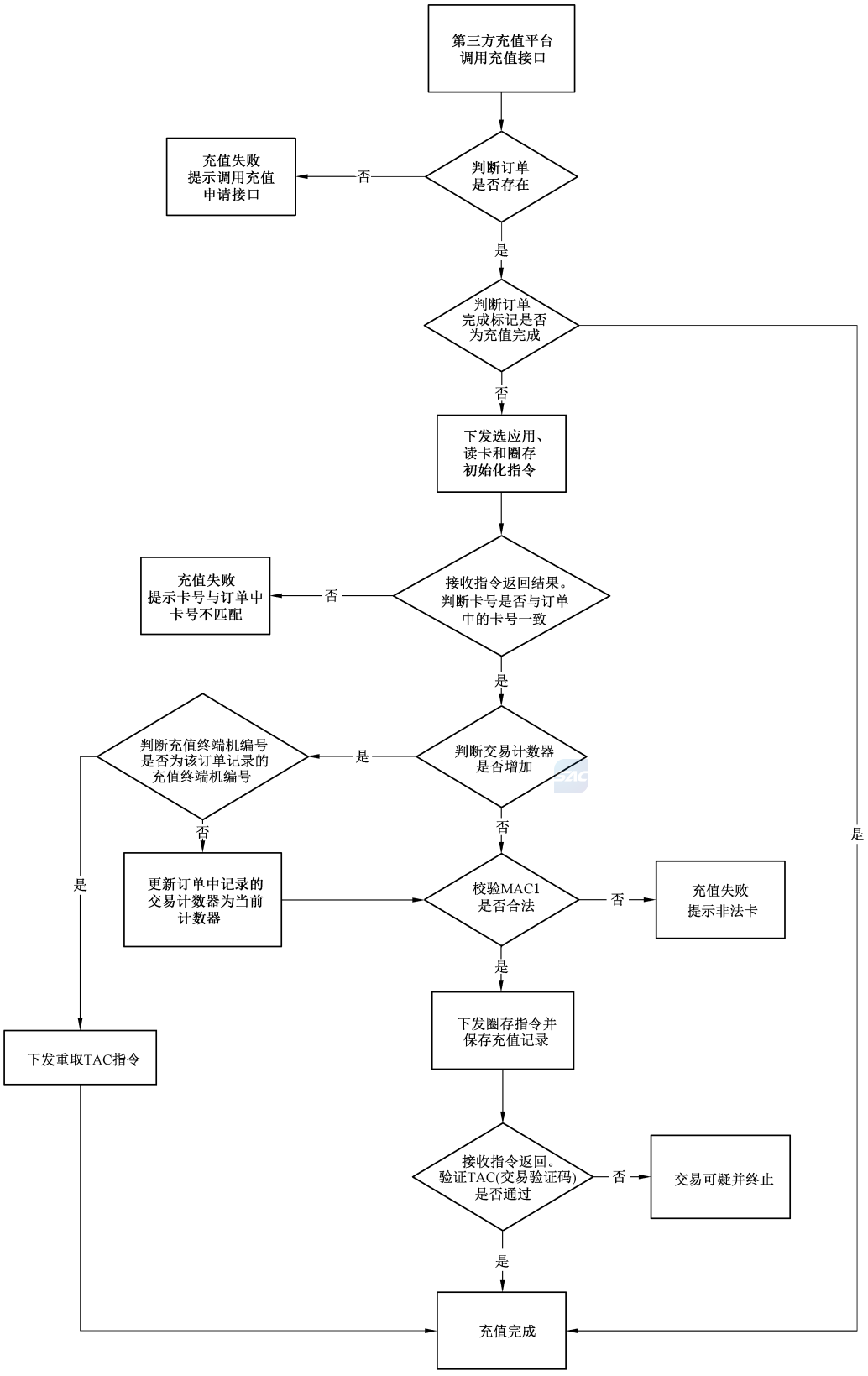

图 4　充值操作流程

充值时序见图 5。

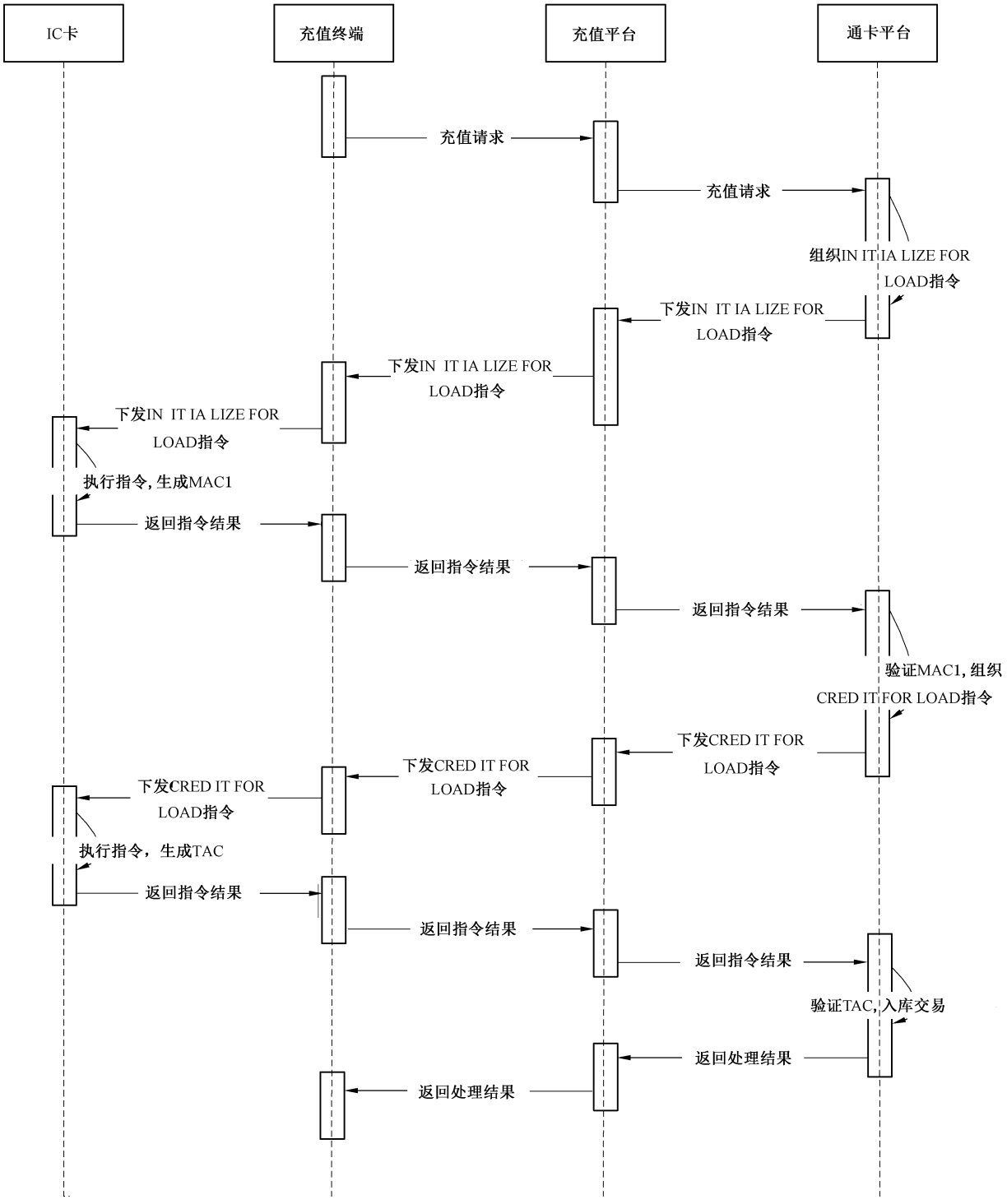

图 5　充值时序图

8.2　流程说明

8.2.1　组织圈存初始化（INITIALIZE FOR LOAD）指令

当充值平台接收到充值终端发起的充值请求时，应组织并下发 INITIALIZE FOR LOAD 指令启

动充值操作。

8.2.2 处理圈存初始化(INITIALIZE FOR LOAD)指令

充值终端接收并转发 INITIALIZE FOR LOAD 指令至 IC 卡,IC 卡将进行下列操作:

a) 检查钱包是否被灰锁。如果灰锁,应回送状态码'9408',但不回送其他信息,同时终止命令的处理过程。
b) 检查是否支持命令中包含的密钥索引号。如果不支持,应回送状态码'9403',但不回送任何其他数据,同时终止命令的处理过程。
c) 产生一个伪随机数,过程密钥和一个报文认证码(MAC1),供通卡后台验证充值操作及 IC 卡的合法性。
d) IC 卡将 INITIALIZE FOR LOAD 响应报文回送给充值终端处理。如果 IC 卡回送的状态码不是'9000',充值操作应终止。

8.2.3 验证报文认证码 1(MAC1)

收到 INITIALIZE FOR LOAD 命令响应报文后,充值终端通过充值平台将响应数据传给通卡后台。通卡后台将生成并确认 MAC1 是否有效。如果 MAC1 有效,充值操作将继续执行。否则,应返回错误状态至充值平台,充值平台通知充值终端中止交易。

8.2.4 组织圈存(CREDIT FOR LOAD)指令

确认充值交易后,充值平台将从持卡人在的相应账户中扣减充值金额,并通知通卡平台。通卡平台产生一个报文认证码 2(MAC2),用于 IC 卡对通卡平台合法性检查。

成功充值交易后,通卡平台将电子存折联机交易序号或电子钱包联机交易序号加 1,并向充值平台发送一个充值交易接受报文,其中包括 MAC2、交易日期和交易时间,充值平台根据报文组织 CREDIT FOR LOAD 指令。

8.2.5 处理圈存(CREDIT FOR LOAD)指令

充值终端收到充值平台 CREDIT FOR LOAD 指令后下发到 IC 卡,更新卡上电子存折或电子钱包余额。

8.2.6 验证报文认证码 2(MAC2)

收到 CREDIT FOR LOAD 命令后,IC 卡应确认 MAC2 的有效性。如果 MAC2 有效,IC 卡将电子存折联机交易序号或电子钱包联机交易序号加 1,并且把交易金额加在电子存折或电子钱包的余额上,IC 卡将根据充值交易信息生成 TAC。否则将向终端回送状态码'9302',充值操作结束,进入异常处理。

8.2.7 返回确认

在 MAC 验证成功后,IC 卡通过 CREDIT FOR LOAD 命令的响应报文将 TAC 回送给充值终端。充值终端将通过充值平台将 TAC 上送给通卡平台,通卡平台验证 TAC 后,向充值平台返回验证结果,若通过,充值平台应通知充值终端充值操作完成,否则应进入充值异常处理。

9 充值异常处理

9.1 一般规定

充值平台对接通卡平台充值异常可包括下列情况:

a） 调用充值接口，没有获得交易应答信息；

b） 调用充值接口，交易应答信息中的返回码，非“0”；

c） 从通卡平台获得的充值指令传至 IC 卡，没有从 IC 卡获得应答代码。

充值平台应根据异常情况，重新发起充值接口的调用，通卡平台在接口调用过程中，根据 IC 卡充值状态进行异常处理，也可调用充值结果查询接口，根据返回结果选择退款或重新发起充值。

充值异常操作时序见图 6。

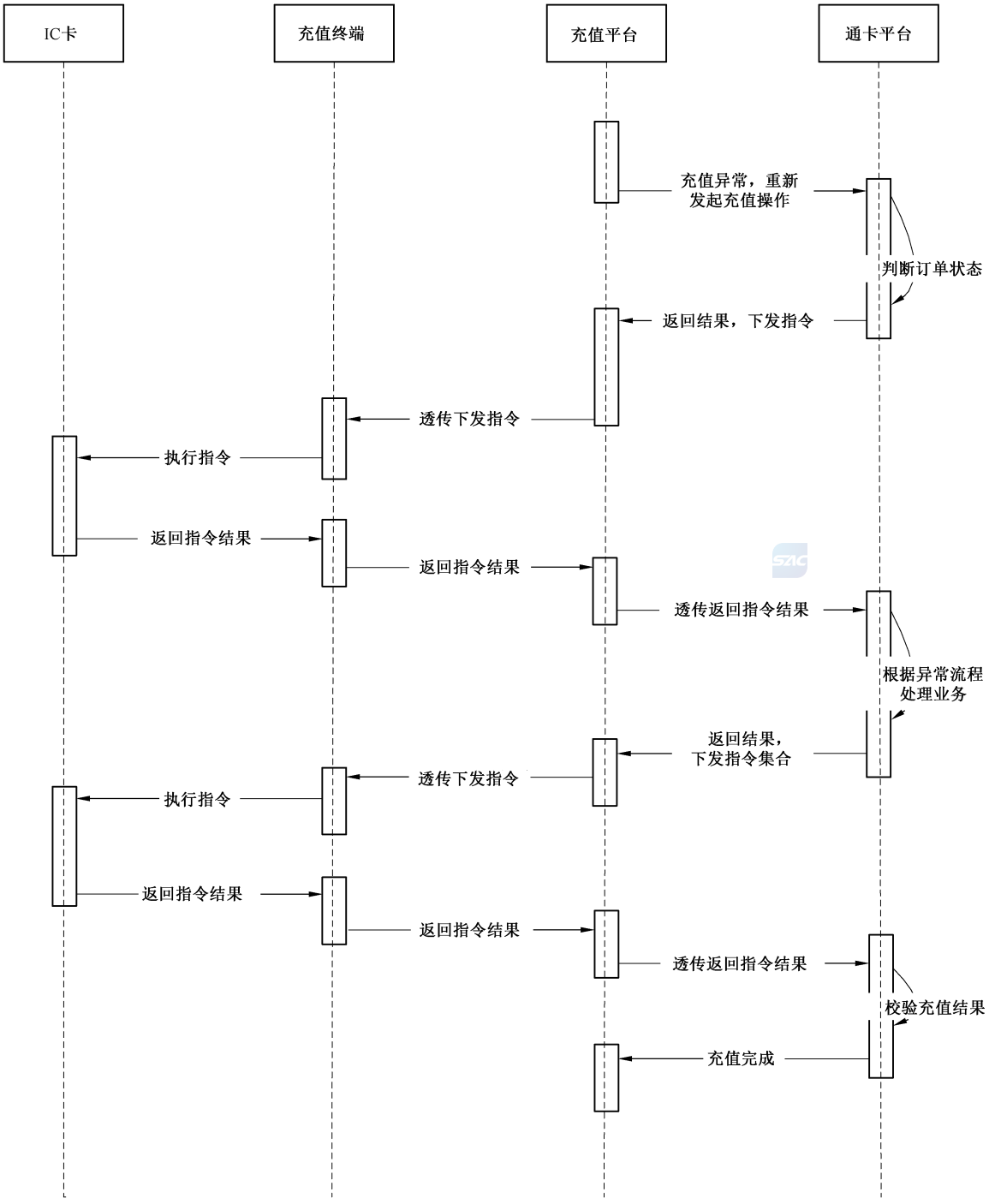

图 6 充值异常操作时序图

9.2 通卡平台异常处理流程

通卡平台下发圈存初始化指令给充值平台，充值平台执行指令并上送指令执行结果。通卡平台针对交易前后IC卡交易计数器的值进行比较，判断流程见图7，并应符合下列要求：

a) IC卡计数器未发生变化：充值失败，继续进行充值流程，校验MAC1成功下发圈存指令，继续完成充值流程；

b) IC卡计数器增加：比较最后一条交易记录的充值终端机编号是否与充值平台该订单使用的充值终端机编号相同，如果相同，证明充值成功，下发获取TAC的指令，完成充值。如果不相同，应更新该订单的交易计数器为当前计数器，校验MAC1成功下发圈存指令，继续完成充值流程；

c) 判断为失败的充值交易，充值平台可选择调用充值结果查询接口，根据返回结果选择退款或重新发起充值，也可不调用充值结果查询接口，直接调用充值接口充值，这时交易日期和时间应变化，以充值成功日期为准；

d) 判断为成功的充值交易，进行正常的清分与结算处理；

e) 判断为可疑的充值交易，由通卡平台的清分部门根据该卡后续的交易情况进行可疑交易调整。调整为成功交易的正常清分与结算处理，调整为失败的交易通知充值平台退款。

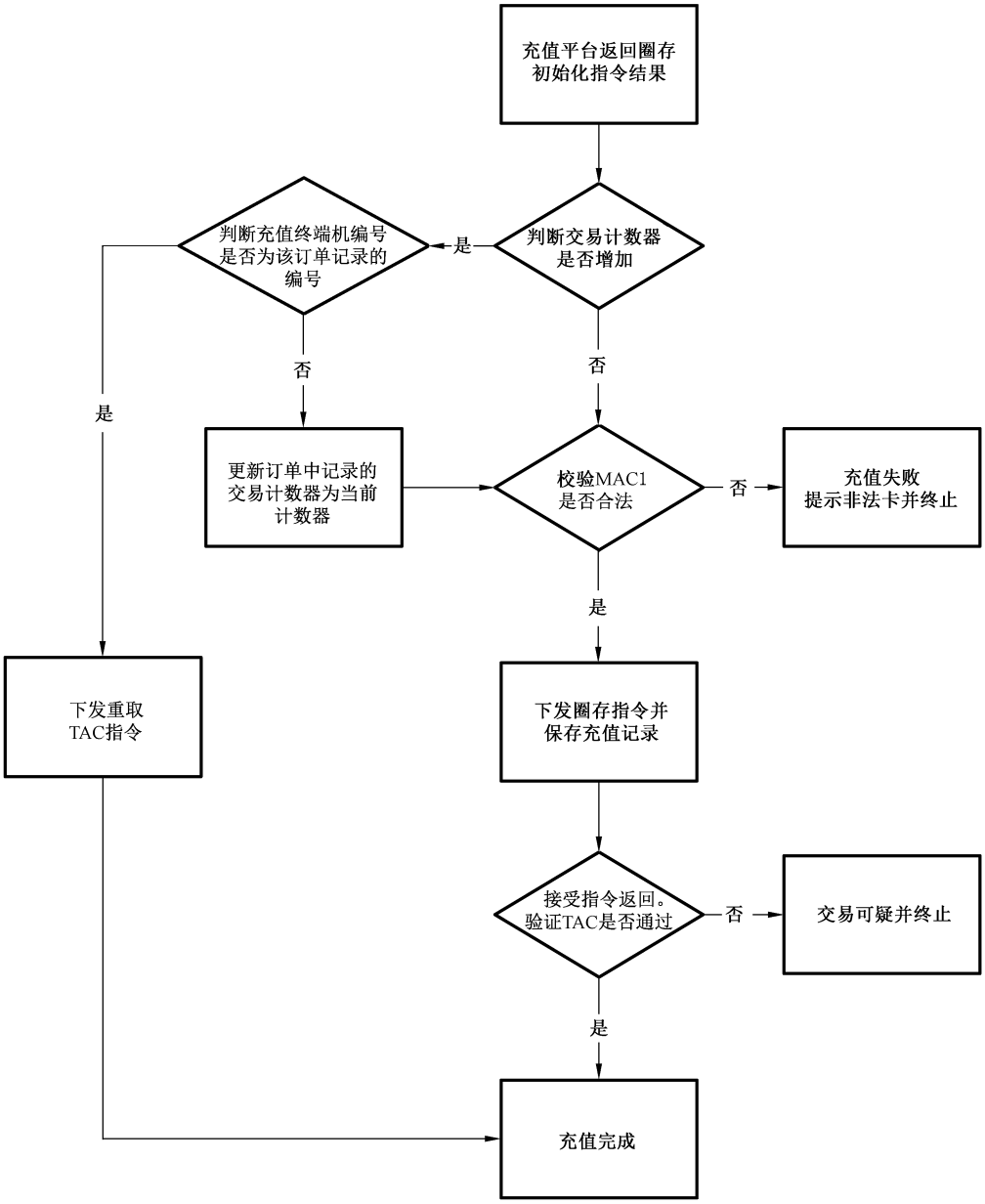

图 7　充值异常判断流程

10　对账文件处理

10.1　一般规定

充值平台和通卡平台对账应符合下列要求：

a）　通卡平台每日生成充值交易明细数据文件，作为对账的依据；

b）　通卡平台只要在充值操作中发出 CREDIT FOR LOAD 指令，即视作充值成功，记录至充值交易明细数据文件；

c）　通卡平台在轧差中如发现以前的充值不成功，应在发现的当日在充值交易明细数据文件中进行结算修正；

d) 如果不一致，双方可协商采用人工对账并查出原因。

10.2 对账流程

对账数据处理流程应符合下列要求：

a) 通卡平台 $T+1$ 日时先对 T 日的实时充值交易的数据统计，根据不同的充值平台生成相应的充值交易明细数据文件，并把数据文件放至指定的 FTP 目录上；

b) 充值平台从不同的通卡平台通过 FTP 获取 $T+0$ 日充值交易明细数据文件；

c) 充值平台按规定格式检查和解析充值交易明细数据文件，并按城市分类对账。

10.3 对账数据备份

对账数据的备份应每天进行当天交易日志的增量备份，定期进行全量数据备份，根据需要进行整个数据库备份。通卡平台和充值平台备份数据应至少保留 3 年。

10.4 充值交易明细数据文件

10.4.1 用途

用于规范地方通卡平台下发的充值交易明细文件，并应符合下列要求：

a) 结算标志为结算成功表示生成该充值交易明细数据文件时地方通卡公司认为成功的交易；

b) 结算标志为结算修正表示地方通卡公司通过清分确认充值失败；

c) 文件内容属于应包含的，通卡公司可增加自定义内容。

10.4.2 命名规则

文件应采用 txt 格式，充值交易明细数据文件命名规则应符合表 2 的规定。

表 2 充值交易明细数据文件命名规则

数据元	数据类型	长度	值
文件标识	String	2	CZ
日期		6	YYMMDD
地方通卡机构代码		8	00000001～99999999
序列号		6	000000～999999
充值平台代码		8	00000001～99999999

10.4.3 文件格式

交易下发包文件格式应符合表 3 的规定。

表 3　充值交易明细数据文件格式

数据元		数据类型	长度	说明
文件说明区	版本号	String	2	01
	交易类型		4	2100(表示充值交易)
	回车符		2	0x0d 和 0x0a
交易头	记录总数		5	取值范围为 00001～99999
	地方通卡公司代码		8	由地方级数据处理系统指定的编号:取值范围为 00000001～99999999
	单笔交易长度		4	包含回车换行:取值范围为 0001～9999
	回车符		2	0x0d 和 0x0a
交易数据	地方通卡公司充值流水号		32	长度不足前补 00
	城市代码(卡属地)		4	卡属地城市代码
	用户卡应用序列号		16	取值范围为 0000000000000001～FFFFFFFFFFFFFFFF
	交易金额		8	单位为分,取值范围为 00000001～99999999
	交易发生日期		8	YYYYMMDD
	交易发生时间		6	HHMMSS
	结算标志		1	0 为结算成功;1 为结算修正
	回车符		2	0x0d 和 0x0a

参 考 文 献

[1] JR/T 0025.2—2010 中国金融集成电路(IC)卡规范 第2部分:电子钱包/电子存折应用规范