ICS 35.240.40
A 11

JR

中华人民共和国金融行业标准

JR/T 0025.13—2018
代替 JR/T 0025.13—2013

中国金融集成电路（IC）卡规范 第13部分：基于借记/贷记应用的小额支付规范

China financial integrated circuit card specifications—Part 13: Low-value payment specifications based on debit/credit application

2018-11-28 发布　　2018-11-28 实施

中国人民银行　发布

目　　次

前　言

JR/T 0025—2018《中国金融集成电路（IC）卡规范》分为14部分：

——第1部分：总则；

——第3部分：与应用无关的IC卡与终端接口规范；

——第4部分：借记/贷记应用规范；

——第5部分：借记/贷记应用卡片规范；

——第6部分：借记/贷记应用终端规范；

——第7部分：借记/贷记应用安全规范；

——第8部分：与应用无关的非接触式规范；

——第10部分：借记/贷记应用个人化指南；

——第12部分：非接触式IC卡支付规范；

——第13部分：基于借记/贷记应用的小额支付规范；

——第14部分：非接触式IC卡小额支付扩展应用规范；

——第15部分：电子现金双币支付应用规范；

——第16部分：IC卡互联网终端规范；

——第18部分：基于安全芯片的线上支付技术规范。

本部分为JR/T 0025—2018的第13部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分代替JR/T 0025.13—2013《中国金融集成电路（IC）卡规范　第13部分：基于借记/贷记应用的小额支付规范》，与JR/T 0025.13—2013相比主要技术变化如下：

——删除“检测具有电子现金功能的金融IC卡的方法由发卡行自定义”（2013年版B.3.3.1）；

——增加了判断卡片是否支持电子现金应用的方法（见表B.1）。

本部分由中国人民银行提出。

本部分由全国金融标准化技术委员会（SAC/TC 180）归口。

本部分起草单位：中国人民银行、中国工商银行、中国银行、中国建设银行、中国农业银行、交通银行、中国邮政储蓄银行、上海浦东发展银行、中国银联股份有限公司、中国金融电子化公司、银行卡检测中心、北京中金国盛认证有限公司、中钞智能卡研究院、中钞信用卡产业发展有限公司、捷德（中国）信息科技有限公司、惠尔丰（中国）信息系统有限公司、福建联迪商用设备有限公司。

本部分主要起草人：李伟、王永红、李晓枫、陆书春、潘润红、李兴锋、宋汉石、渠韶光、邵阔义、杨倩、聂丽琴、杜宁、周玥、张宏基、程胜、汤沁莹、黄本涛、陈则栋、吴晓光、李春欢、洪隽、张栋、王红剑、刘志刚、张永峰、胡吉晶、吴潇、范抒、魏猛、余沁、尚可、李新、李一凡、周新衡、邓少峰、张步、冯珂、李建峰、向前、涂晓军、林发全、陈文博、石文鹏、齐大鹏、陈震宇、郑元龙、聂舒、丁吉、白雪晶、李子达、沈卓群、刘世英、于海涛、翁秀诚、张萌、熊涛、陈泽智、谭世殊、吴孟晴、万兵、董凌骏、黎志勇、袁国能、张国栋、俞益宁、曾静静、李铭铭、梁玮韬、章盼、张波波、汪小八、拱慧璇、柳姣娜。

本部分代替JR/T 0025.13—2013。

JR/T 0025.13—2013的历次版本发布情况为：

JR/T 0025.13—2010。

引　言

本部分为JR/T 0025—2018的第13部分，与JR/T 0025.4—2018至JR/T 0025.7—2018一起构成基于借记/贷记的小额支付应用。

本部分主要定义了与小额支付有关的内容，即小额支付的技术实现与所支持的交易类型等。本部分未特别说明的内容，与标准借记/贷记应用一致，相关要求在JR/T 0025.4—2018至JR/T 0025.7—2018中描述。

中国金融集成电路（IC）卡规范
第13部分：基于借记/贷记应用的小额支付规范

1 范围

本部分规定了关于如何在借记/贷记卡上实现小额支付功能（即电子现金）的相关信息，并提供了电子现金的功能概述，包括卡片应用程序、终端功能与发卡行系统的示例等，发卡行后台的账户处理不在本部分范围之内。

本部分适用于银行发行和受理的具有小额支付功能的借记/贷记金融IC卡。使用对象主要是与金融借记/贷记IC卡应用相关的卡片设计、制造、管理、发行、受理以及应用系统的研制、开发、集成和维护等相关部门（单位）。

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。

JR/T 0025—2018（所有部分） 中国金融集成电路（IC）卡规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

持卡人验证方法 cardholder verification method

验证持卡人是否合法的方法，终端用他来确保卡片不是丢失的或被盗的。

3.2

清算 clearing

发卡行针对收单行提交的交易数据进行的处理过程。

注：对于发卡行来说，清算是将后台计数器与卡中计数器进行再同步的一次机会。对于收单行来说，清算是将交易数据上送给发卡行。

3.3

命令 command

终端向IC卡发出的一条报文，该报文启动一个操作或请求一个响应。

3.4

密文 cryptogram

加密运算的结果。

3.5

电子现金（EC） electronic cash（EC）

基于借记/贷记应用上实现的小额支付功能。

3.6

电子现金余额 electronic cash balance

一个计数器，表示卡片上可脱机消费的金额。

3.7

电子现金余额上限 electronic cash funds limit

持卡人可用来脱机消费的最大金额。

3.8

发卡行行为代码 issuer action code

发卡行根据TVR的内容选择的动作。

3.9

圈存 load

增加卡中电子现金余额的过程。圈存有多种实现方式，可以从主账户中划入金额，也可以现金存款，又或者从其他账户转入金额，但圈存后的电子现金余额不能超过电子现金余额上限。

3.10

磁条 magstripe

包括磁编码信息的条状物。

3.11

响应 response

IC卡处理完收到的命令报文后，返回给终端的报文。

3.12

脚本 script

发卡行向终端发送的命令或命令序列，目的是向IC卡连续输入命令。

3.13

终端 terminal

在交易点安装的用于与IC卡配合共同完成金融交易的设备，应包括接口设备，也可包括其他的部件和接口（如与主机的通讯）。

3.14

交易日志 transaction log

记录最近交易的信息细节，从中可以了解交易历史。

3.15

圈提 unload

减少卡中电子现金余额至零的过程。

注：圈提的结果将电子现金账户中全部余额转入卡片主账户或以等额的现金返还给持卡人。圈提用于持卡人或发卡行取消电子现金功能。

4 缩略语

下列缩略语适用于本文件。

AAC——应用认证密文（Application Authentication Cryptogram）
AFL——应用文件定位器（Application File Locator）
AIP——应用交互特征（Application Interchange Profile）
ARPC——授权响应密文（Authorization Response Cryptogram）
ARQC——授权请求密文（Authorization Request Cryptogram）
ATC——应用交易计数器（Application Transaction Counter）
AC——应用密文（Application Cryptogram）
ARQC——授权请求密文（Authorization Request Cryptogram）
ATM——自动柜员机（Automated Teller Machine）
CAM——卡片认证方法（Card Authentication Method）
CDOL——卡片风险管理数据对象列表（Card risk Management Data Object List）
CVM——持卡人验证方法（Cardholder Verification Method）
EC——电子现金（Electronic Cash）
IC——集成电路（Integrated Circuit）
IDD——发卡行自定义数据（Issuer Defined Data）
PIN——个人识别码（Personal Identification Number）
TC——交易证书（Transaction Certificate）
POS——销售点（Point Of Sale）
SW1——状态字1（Status Word One）
SW2——状态字2（Status Word Two）

5 卡片及终端技术要求

5.1 新增数据元

在借记/贷记应用的基础上新增的数据元，见表1和表2。

表1 卡片数据元

数据元名称	获取	标签	长度	格式
电子现金余额（EC Balance）	Get Data	9F79	6	n 12
电子现金余额上限（EC Balance Limit）	Get Data	9F77	6	n 12
电子现金发卡行授权码（EC Issuer Authorization Code）	Read Record	9F74	6	a
电子现金单笔交易限额（EC Single Transaction Limit）	Get Data	9F78	6	n 12

数据元名称	获取	标签	长度	格式
电子现金重置阈值（EC Reset Threshold）	Get Data	9F6D	6	n 12
圈存日志入口	Select	DF4D	2	b 16
圈存日志格式	Get Data	DF4F	可变	b

部分数据元的说明如下：

——电子现金余额：该数据元保存了可供脱机消费的剩余总额。对于每一笔成功的电子现金交易，卡片从中减去相应的授权金额，一旦授权金额超过了电子现金余额，则卡片按照标准借记/贷记处理该笔交易；

——电子现金余额上限：表示在电子现金应用中，持卡人可脱机消费的最大累积额度，即卡片充值所能达到的上限，发卡行可修改此上限值；

——电子现金发卡行授权码：卡片上用于标识批准电子现金交易的代码，在脱机批准交易中，该代码被存放在清算报文的授权码中，格式为“ECCxxx”，其中“xxx”是发卡行定义的编号；

——电子现金单笔交易限额：卡片上单笔电子现金授权金额的上限，用于控制单笔电子现金交易风险，在个人化时由发卡行写入，并可由发卡行重新设置；

——电子现金重置阈值：触发卡片进行自动圈存的余额下限，当卡片上的电子现金余额小于该阈值时，终端即请求联机，发卡行可对该交易下发发卡行脚本，以完成自动圈存。

表2　终端数据元

数据元名称	标签	长度	格式
电子现金终端支持指示器（EC Terminal Support Indicator）	9F7A	1	b
电子现金终端交易限额（EC Terminal Transaction Limit）	9F7B	6	n 12

数据元的说明如下：

——电子现金终端支持指示器：指示该终端支持电子现金处理；

——电子现金终端交易限额：终端使用此数据元（如果存在的话）判断交易是否以电子现金方式处理。若存在此数据元，当授权金额大于等于此限额时，终端将电子现金终端支持指示器的值置为零，并不将该交易作为电子现金交易处理；若不存在此数据元，当授权金额大于等于终端最低限额（9F1B）时，终端将电子现金终端支持指示器的值置为零，并不将该交易作为电子现金交易处理。

5.2　卡片脱机数据认证

卡片脱机数据认证的描述见JR/T 0025.7—2018。

发卡行应采用强有力的CAM机制，以防止脱机欺诈的风险，如在个人化时将卡片设置为只有在执行动态数据认证（DDA）或复合动态数据认证/应用密文生成（CDA）的情况下允许脱机交易，AIP应参与静态数据签名。

5.3　持卡人验证方法原则

CVM列表设置宜按照以下原则进行设置：

为实现脱机处理，联机 PIN 不能设为首选 CVM。

5.4　交易日志

电子现金功能采用与借记/贷记同样的方式记录交易日志。

5.5　货币转换

电子现金余额是以应用货币计算的可用于脱机消费的值。无论对卡还是终端，电子现金功能均不允许支持货币转换，因为电子现金余额应准确反映可供消费额，而货币转换可能导致卡中保存不准确的电子现金余额值。

5.6 数据元的使用

如5.1描述，电子现金新增了电子现金余额、电子现金余额上限和电子现金单笔交易限额三项卡片数据元，以管理发卡行的脱机风险。

发卡行可以根据脱机计数器的界限值改变卡的行为。卡片风险管理按如下方式使用这些界限值：

——如果授权金额小于或等于电子现金余额且小于或等于电子现金单笔交易限额，则卡片批准脱机交易；

——当授权金额的值超出电子现金余额或电子现金单笔交易限额时，进行标准借记/贷记流程处理。

发卡行可以根据持卡人已脱机消费的额度和持卡人主账户余额，对交易进行联机授权。发卡行可通过脚本的方法进行充值以调整电子现金余额值，见本部分第8章。

5.7 脚本

脚本实现的详细信息见JR/T 0025.5—2018。

5.8 圈存日志

圈存日志是区别于交易日志的独立日志，他由卡片负责记录并保存。当卡片中的电子现金余额被设置数据命令（Put Data）成功改写时，卡片应记录一条圈存日志。

交易日志的记录、循环覆盖不应影响到圈存日志，反之亦然。

记录圈存日志与设置数据命令（Put Data）应同时成功。若二者之一失败，则另一个操作应同时失败。

圈存日志记录文件是一个定长循环记录文件。该文件的短文件标识符和记录个数在圈存日志入口（DF4D）中规定。DF4D的第一个字节定义了圈存日志记录文件的短文件标识符，圈存日志记录文件的短文件标识符取值范围应在11-30之间，且不与JR/T 0025—2018中定义的其他文件重复，JR/T 0025—2018圈存日志的短文件标识符宜为12（即0x0C），圈存日志入口应在选择应用的时候，由卡片在ADF的FCI中的BF0C模板中返回。DF4D的第二个字节定义了圈存日志记录个数。卡片应支持至少存储十条圈存日志。

圈存日志的内容在本部分第10.2条中定义。

圈存日志格式（DF4F）和圈存日志记录在应用锁定后应仍可以被访问。

圈存日志信息的读取包括逐条读取圈存日志信息和一次性读取全部圈存日志信息两种：逐条读取圈存日志信息可用于持卡人或发卡行查询圈存明细；一次性读取全部圈存日志可用于在自助设备或者发卡行柜台获取由MAC保护的完整圈存日志，以便发生账户差错时为调账提供参考。两种方式分别使用下列步骤：

——逐条读取：

- 执行应用选择，在 FCI 的发卡行自定义数据处获得圈存日志入口数据元。如果圈存日志入口不存在，则表明该界面下应用不支持圈存日志读取功能；
- 发送一个取数据命令（GET DATA）取得圈存日志格式；
- 发送读记录命令（READ RECORD）（P1=记录号）读圈存日志记录。

——一次性读取全部圈存日志：

- 执行应用选择，在 FCI 的发卡行自定义数据处获得圈存日志入口。如果圈存日志入口不存在，则表明该界面下应用不支持圈存日志读取功能；
- 发送读记录命令（READ RECORD）（P1=00）读圈存日志记录；

- 圈存日志记录文件的读权限为自由读，写权限不公开，由卡片操作系统控制。

当非接触应用选择的FCI中未个人化圈存日志入口时，卡片应不允许通过非接触界面读取圈存日志，此时当卡片收到读取圈存日志的READ RECORD命令时，应返回6A82。

除发卡行有特殊业务需求外，非接触界面下FCI信息中不应包含圈存日志入口，以保证圈存日志信息不在非接触界面下被读取。否则，如造成持卡人隐私泄露，由发卡行承担相应责任。

6 余额的含义

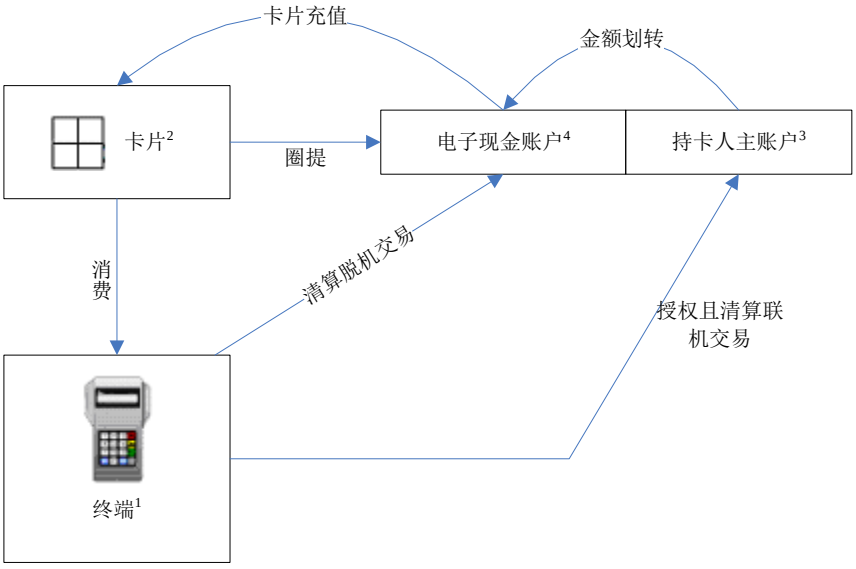
使用术语“余额”并不表示卡中具有货币，而是表示发卡行承诺给商户的最高脱机支付金额。除电子现金余额外，可能存在不同数值的“余额”，例如：主账户余额：用于借记/贷记交易的最大可支付额度，此为主账户中的可用余额。

发卡行应对其持卡人作相应的培训，使其了解在不同的情况下可能造成不同的可供消费余额。

7 功能模式

7.1 电子现金功能模式组成

图1展示了电子现金功能模式的不同组成部分。



注1：“终端”是指任何与 JR/T 0025—2018 借记/贷记应用兼容的金融 IC 卡终端，可支持或不支持进行联机交易。

注2：“卡片”是指运行符合 JR/T 0025—2018 借记/贷记应用程序并个人化、能执行电子现金交易的金融 IC 卡。

注3：“持卡人主账户”假定为用于联机授权的当前账户。

注4：“电子现金账户”中预先保留了电子现金金额，用于：

——防止电子现金金额用于非电子现金支付；

——对卡脱机交易进行清算。

图1 电子现金功能模式

7.2 电子现金账户

发卡行实现电子现金应用时，为每张卡设置一个授权消费的最大额度。该额度因卡而异，且由发卡行内部管理，发卡行用于管理该额度的账户称为“电子现金账户”。

在发卡行主机系统中，可将电子现金账户当成一个独立账户管理。持卡人可按如下方式将金额转移至电子现金账户[1)]：

——主账户转账；

——现金充值；

——第 3 方转账。

可能会由于以下原因导致电子现金账户金额与电子现金余额两个金额值之间的差异：

——交易执行与发卡行受理并对交易记录进行清算之间的延迟；

——发卡行对电子现金账户圈存，与对金融 IC 卡电子现金余额的更新（通过发卡行脚本命令，需要卡与发卡行双向在线互联进行）之间的延迟；

——异常处理。

对电子现金产品的实际配置将决定哪种余额为准确值，本章后续的内容将予以解释。

7.3 电子现金账户金额和卡余额的初始设定

当持卡人初始设立一个与具有电子现金功能的金融IC卡关联的账户时，将通过7.2提供的方法提供一定的初始金额，以创建电子现金账户金额，发卡行创建该账户并向持卡人发卡。个人化阶段可将卡中电子现金余额设为该初始金额值。

另一种选择是发卡行可以将卡中电子现金余额设为“0”，并安排后续的圈存交易来充入金额。

7.4 交易

圈存交易包括了资金转移和卡充值交易两步：第1步将资金转移至电子现金账户中，第2步通过充值交易将电子现金账户的金额同步到卡的电子现金余额。

消费交易一般由卡片进行脱机授权，与这些交易相关的清算操作使用电子现金账户。因此，圈存操作使电子现金账户金额增加，脱机交易清算使电子现金账户金额减少。

所有联机消费交易通常针对持卡人主账户进行授权和清算，既不影响电子现金账户金额，也不影响卡中电子现金余额。

圈提交易用于将卡中全部的电子现金余额划入卡的主账户并将卡片中的电子现金余额清零，或者用等额现金返还持卡人。

交易中电子现金余额和电子现金额度的变化参见附录A。

具体操作步骤参见附录B。

7.5 交易处理

7.5.1 应用选择

终端发送SELECT命令选择应用，卡片返回文件控制信息（FCI），其中包括了请求电子现金终端支持指示器（9F7A）、授权金额（9F02）以及交易货币代码（5F2A）的PDOL。

7.5.2 初始化应用

如果满足以下条件：

1) 发卡行应知道的是，电子现金账户金额是用于分配给脱机交易使用，且未提交清算的金额值。所有脱机授权的交易针对电子现金账户金额清算。因此，电子现金账户金额并非总是精确反映出卡片当前电子现金余额。这些值均无必要。

——终端支持电子现金交易；
——授权金额小于电子现金终端交易限额，或者在终端不包括单独的电子现金终端交易限额的情况下，小于终端最低限额；
——终端交易类型为消费交易。
那么，终端将在GPO命令中提供电子现金终端支持指示器（设置为“1”）。
当收到GPO命令时，如果以下条件满足，卡片将此交易看作一个电子现金交易：
——命令中包含电子现金终端支持指示器（设置为“1”）；
——交易货币代码与应用货币代码匹配；
——授权金额不超过电子现金余额；
——授权金额不超过电子现金单笔交易限额；
——发卡行认证失败指示器为“0”；
——上次联机交易发卡行脚本处理失败指示器为“0”；
——PIN 尝试次数不为“0”。
如果以上任一条件不满足，交易就不是一个电子现金交易。
如果此次交易被卡片看作是一笔电子现金交易，那么卡片应：
——标识本次交易为电子现金交易；
——返回 GPO 响应数据 AIP 和 AFL，AIP 指示电子现金交易支持的功能，AFL 则指明了电子现金特定数据（电子现金发卡行授权码的位置）。
如果此次交易不是电子现金交易，卡片在GPO的响应中返回非电子现金的AIP和AFL（不返回电子现金发卡行授权码），终端将此交易当作标准借记/贷记交易处理。
当终端收到AIP和AFL，且电子现金发卡行授权码存在，则用GET DATA命令读取如下数据：
——电子现金余额；
——电子现金重置阈值。
如果终端没有收到AIP和AFL，则交易被终止。

7.5.3 终端风险管理

终端不进行最低限额、随机交易选择和频度检查。

7.5.4 终端行为分析

终端从卡片返回的AFL中读取数据，将电子现金余额与授权金额的差值和电子现金重置阈值进行比较，同时结合终端能力进行终端行为分析，具体如下：
——若电子现金余额减去授权金额大于或等于电子现金重置阈值，则本次向卡片请求脱机批准，进行电子现金交易；
——若电子现金余额减去授权金额小于电子现金重置阈值，根据终端能力进行如下判断：
- 若终端具备联机能力，则终端请求联机，并要求持卡人输入联机 PIN，本交易请求发卡行联机授权同时对电子现金余额进行更新；
- 若终端不具备联机能力，则终端请求脱机批准，本交易可以脱机完成；
- 若终端尝试联机失败后，终端和卡进行标准借记/贷记交易处理。

7.5.5 卡片行为分析

对在初始化应用阶段被指明为电子现金的交易而言，卡片执行以下步骤：
——若终端脱机拒绝交易（请求 AAC），卡片在 GENERATE AC 命令响应中返回 AAC；
——跳过联机授权未完成检查、上次交易发卡行认证失败检查、上次联机交易发卡行脚本处理检查、

新卡检查、脱机 PIN 尝试次数检查及各类频度检查，进行上次交易 SDA 失败检查和上次交易 DDA 失败检查；

——若终端请求联机交易，卡片在 GENERATE AC 响应中返回 ARQC；

——若终端请求脱机批准，则卡片应检查终端在 GENERATE AC 命令中给出的标签的值与 GPO 命令中给出的标签的值是否一致（这些标签包括但不仅限于交易货币代码‘5F2A’、授权金额‘9F02’，但不包括终端验证结果‘95’，交易状态信息‘9B’和不可预知数‘9F37’）。如果检查的结果为一致，则卡片从电子现金余额中扣除授权金额并在 GENERATE AC 命令响应中返回 TC，否则卡片在 GENERATE AC 命令响应中返回 AAC；

——在发卡行应用数据（标签 9F10）的发卡行自定义数据（IDD）（见表 3）中返回更新后的电子现金余额；

——电子现金交易的结果，不影响标准借记/贷记中各类计数器的值（ATC 除外）。

7.5.6 结束交易

终端在交易结束时，显示给持卡人的电子现金余额和打印在凭条上的电子现金余额均应从卡片在GAC响应数据中返回的发卡行应用数据（9F10）中的发卡行自定义数据（IDD）中获取，发卡行自定义数据（IDD）的格式见表3。如果发卡行自定义数据（IDD）中不含有电子现金余额，则终端应通过附录C中定义的方法获取电子现金余额。

完成交易后，终端会收集交易数据，通常会在当天营业结束时把交易明细发送给收单行，以进行后续的清算。终端在清算报文的授权码中提供电子现金发卡行授权码。凭据上可以打印出由卡片发送给终端的电子现金余额。

当发卡行接收到用于清算的交易数据时，可识别出交易是否使用电子现金交易，若是，则从电子现金账户（而非持卡人主账户）中扣减相应的交易金额。

表3 发卡行自定义数据（IDD）

IDD 选项	长度（字节）	ID	金额域	MAC 字节数
电子现金余额	10	0x01	标签“9F79”的值。 （低 5 位字节）	4

被进行验证码计算的数据包括两个字节的应用交易计数器，电子现金余额和一个字节0x00的补位。

四字节的验证码是通过从MAC UDK分散的过程密钥计算得来的，数据填充方式见表4。密钥分散方法和MAC计算方法在JR/T 0025.7—2018中定义。

发卡行自定义数据（IDD）由发卡机构在个人化时决定，发卡行自定义数据（IDD）其他定义见JR/T 0025.12—2018附录D。

表4 MAC 计算

ID	数据块长度	元素	
0x01	8 位 bytes	ATC	2 字节
		电子现金余额	低 5 位字节
		填充	1 字节

7.6 交易流程图

交易流程见图2和图3所示。

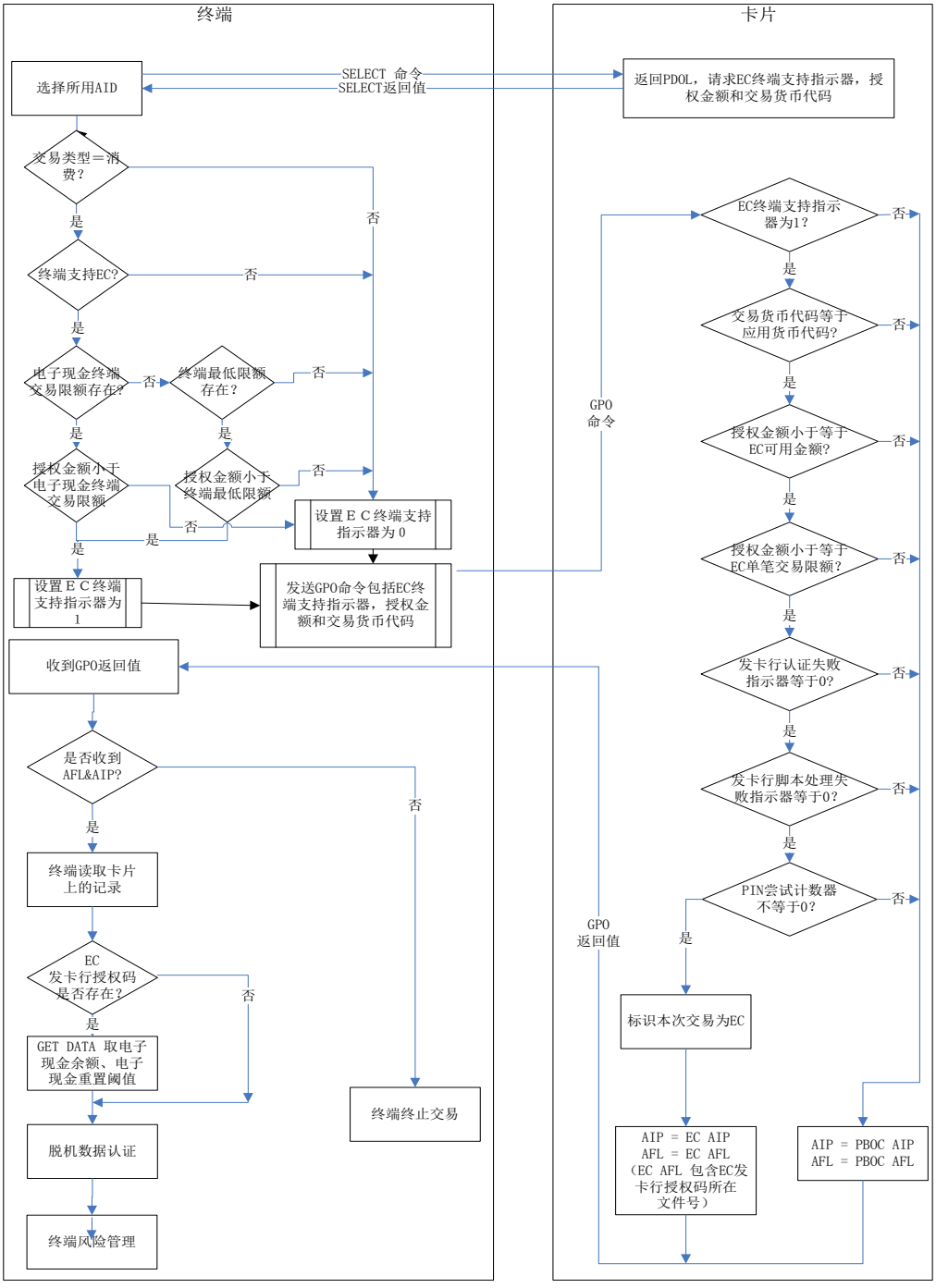
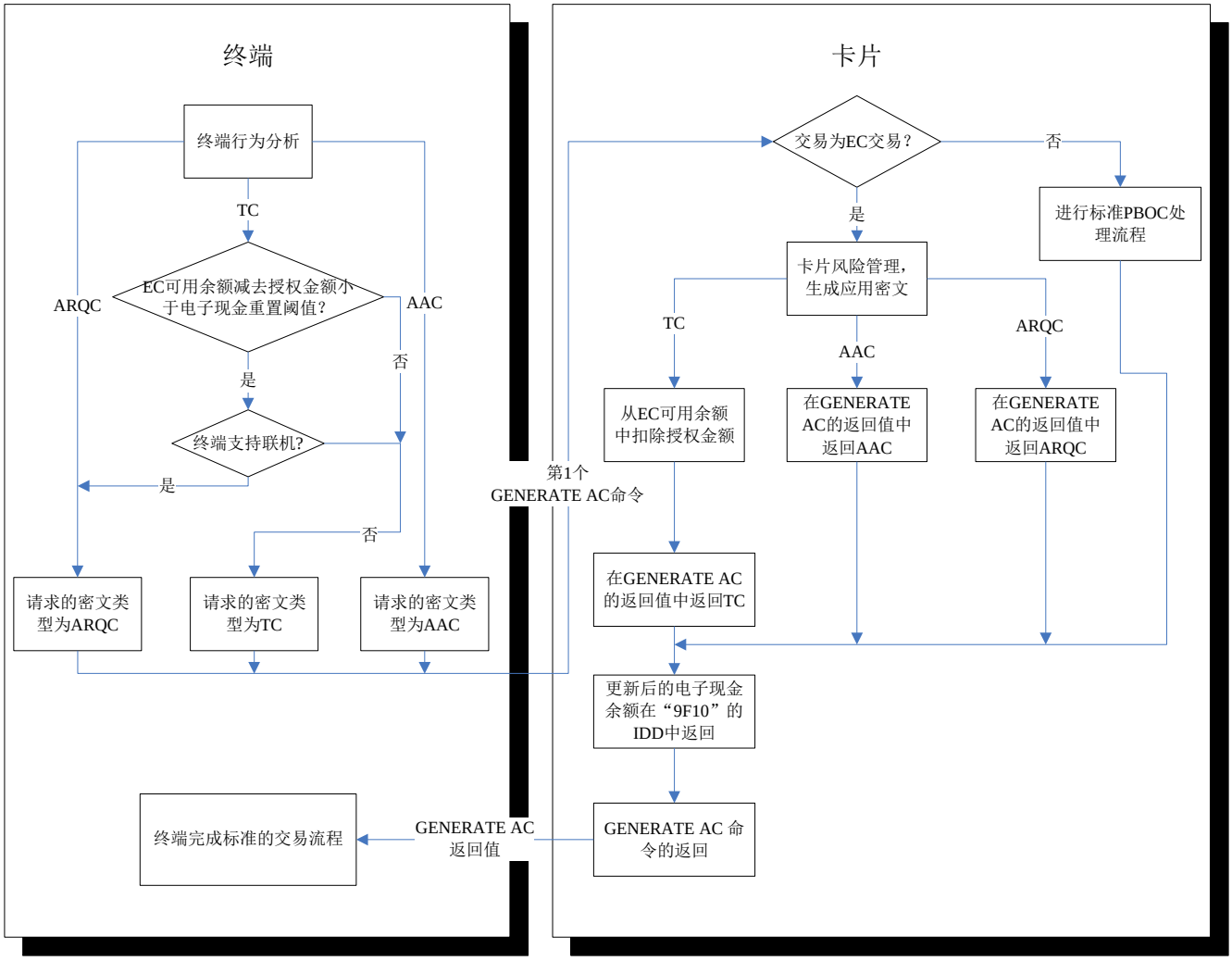

终端
卡片
选择所用AID
SELECT 命令
SELECT返回值
返回PDOL，请求EC终端支持指示器，授权金额和交易货币代码
交易类型＝消费？
是
否
终端支持EC?
否
是
电子现金终端交易限额存在?
否
终端最低限额存在？
否
是
是
授权金额小于电子现金终端交易限额
授权金额小于终端最低限额
否
否
是
是
设置ＥＣ终端支持指示器为0
设置ＥＣ终端支持指示器为1
发送GPO命令包括EC终端支持指示器，授权金额和交易货币代码
GPO命令
收到GPO返回值
是否收到AFL&AIP?
否
是
终端读取卡片上的记录
EC发卡行授权码是否存在?
否
是
GET DATA 取电子现金余额、电子现金重置阈值
脱机数据认证
终端风险管理
终端终止交易
EC终端支持指示器为1?
否
是
交易货币代码等于应用货币代码?
否
是
授权金额小于等于EC可用金额?
否
是
授权金额小于等于EC单笔交易限额?
否
是
发卡行认证失败指示器等于0?
否
是
发卡行脚本处理失败指示器等于0?
否
是
PIN尝试计数器不等于0?
否
是
GPO返回值
标识本次交易为EC
AIP = EC AIP
AFL = EC AFL
（EC AFL 包含EC发卡行授权码所在文件号）
AIP = PBOC AIP
AFL = PBOC AFL

图2　交易流程图（1）



终端按照借记/贷记应用流程继续进行处理

图3　交易流程图（2）

8　调整电子现金余额

在进行若干笔脱机电子现金交易后，卡上的电子现金余额会不断减少，当减少到一定程度时（例如余额小于电子现金重置阈值），脱机电子现金交易便无法进行。这时需要通过联机给卡片进行充值，以重新设置电子现金余额值。这个过程是通过圈存交易来进行的，目前本部分支持手工圈存和自动圈存两种方式，参见B.3。

如果要更新的电子现金余额大于电子现金余额上限，卡片对更新数据命令（Put Data）应返回失败。如果更新电子现金余额成功，卡片应记录一条圈存日志。圈存日志的要求见本部分的5.8和10.2。

9　主机逻辑实现示例

9.1 脱机交易

脱机交易期间，卡使用其内部风险管理判断该次交易是否可脱机授权。卡将当前授权金额与电子现金余额比较，如果当前授权金额超出卡片的电子现金余额，应请求联机授权。

如果交易被脱机批准，卡将从电子现金余额中减去此次交易的授权金额。如果卡请求联机授权但终端不支持联机功能，则进行标准的借记/贷记交易处理。

脱机交易对发卡行系统没有影响。对于脱机交易来说，发卡行可修改其主机系统，以便在清算操作时执行更多的检查。如检查收到的应用交易计数器（ATC），看是否有未完成的交易待提交清算。

9.2 联机交易

导致交易需联机进行的原因有：

——电子现金余额与授权金额的差值小于电子现金重置阈值；

——交易过程中异常发生，强制交易联机进行（如持卡人未能输入正确的脱机 PIN）。

一般情况下，联机后，主机系统会针对电子现金账户，执行与其他金融IC卡授权相同的处理，包括：

——检查卡是否挂失；

——通过验证在 55 域中发送的 ARQC，执行联机 CAM；

——检查芯片数据内容，以发现交易被送至联机的原因。

是否需要的额外处理，取决于交易被送至联机的原因，可能由于电子现金余额不足，或者由于错误的PIN输入等其他原因。发卡行主机系统将根据交易被送至联机进行的原因，进行不同的授权操作。

授权金额大于卡的电子现金余额，则交易将被送至联机，这是最常见的导致交易被送至联机进行的原因。相应的授权处理方式由发卡行自定，主机将执行发卡行在其授权处理中定义的任何额外测试与检查。

在以下两种情景中，主机系统的操作结果见示例1、示例2：

——交易针对持卡人主账户授权。检查主账户余额，如果余额充足，则交易被批准，主机系统将授权批准发回给卡，并从主账户中支出，而卡的电子现金余额保持不变（见“示例 1：针对主账户交易授权，授权金额为 20 元”）；

——发卡行对持卡人电子现金账户进行自动圈存。发卡行可在每次卡获得联机交易机会时，或者仅当电子现金余额低于电子现金重置阈值时，激活“自动圈存”过程（见示例 2：联机授权期间，发卡行对电子现金余额自动圈存至 50 元）。

示例1：针对主账户交易授权，授权金额为20元。

电子现金余额与主账户余额变化见图4、图5和图6所示。

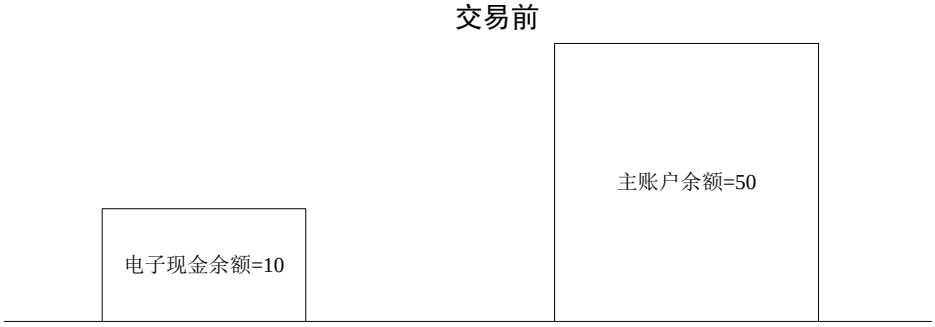


图4 主账户交易授权示例（1）

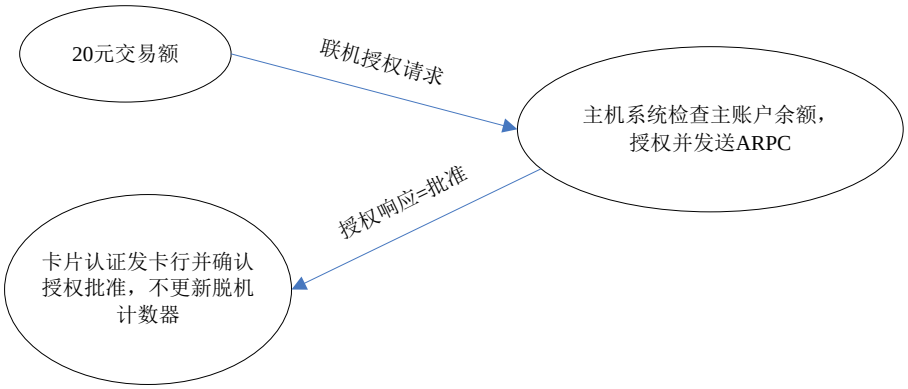


图5　主账户交易授权示例（2）

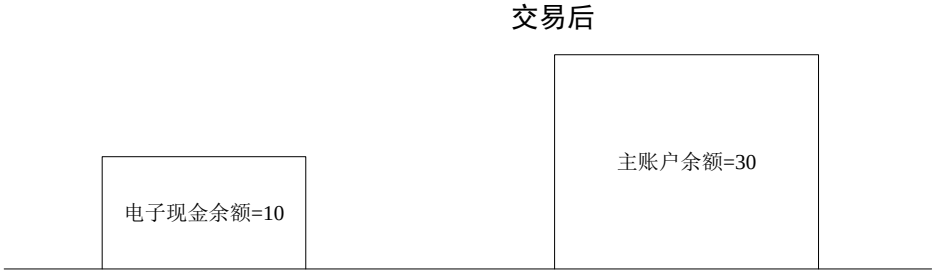


图6　主账户交易授权示例（3）

示例2：联机授权期间，发卡行对电子现金余额自动圈存至50元。

电子现金余额和主账户余额变化如图7、图8、图9、图10和图11所示。

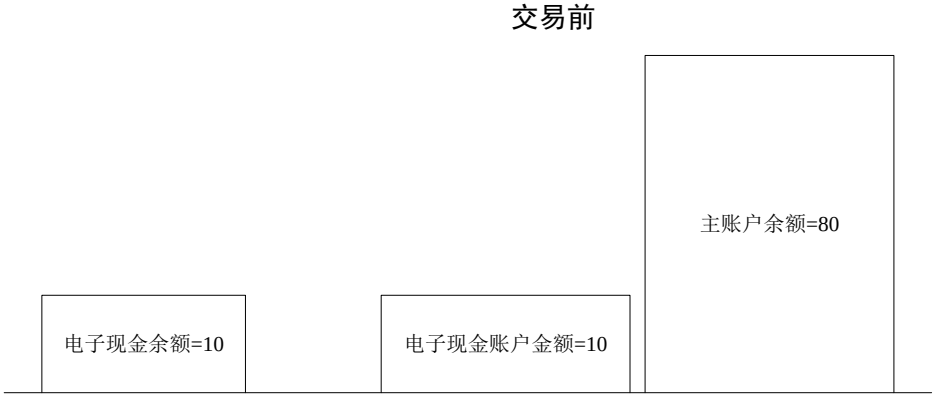


图7　自动圈存示例（1）

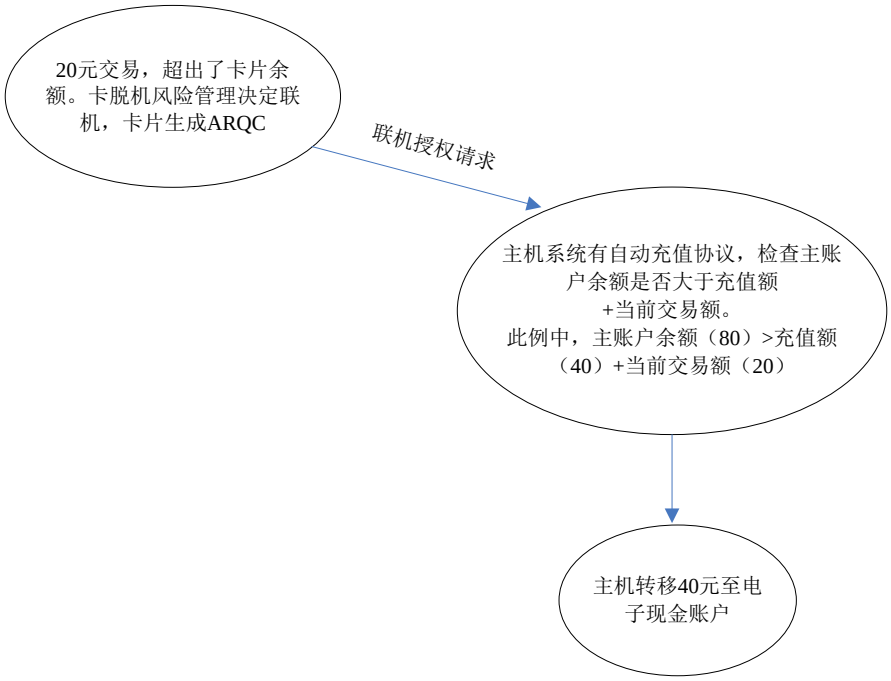


图8　自动圈存示例（2）

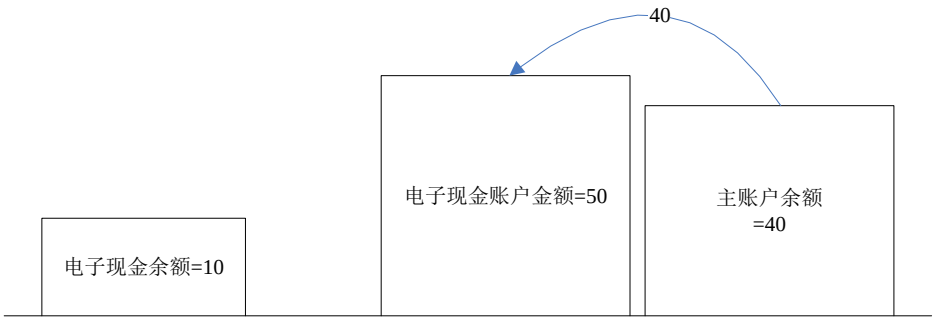


图9　自动圈存示例（3）

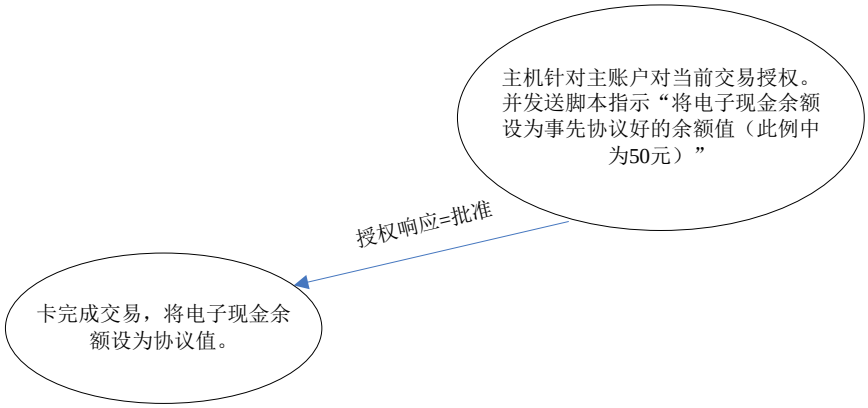


图10　自动圈存示例（4）

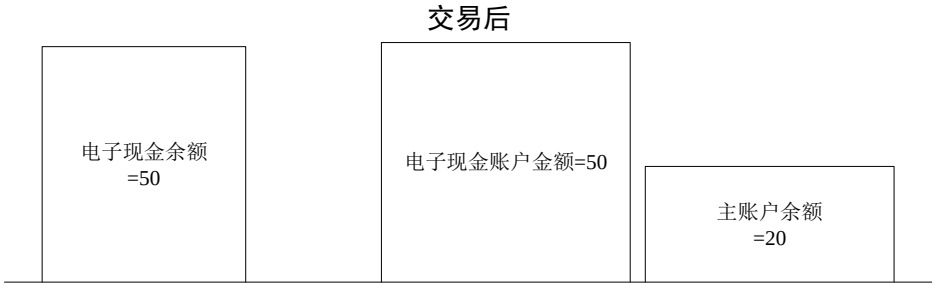


图11　自动圈存示例（5）

10　卡命令

10.1　电子现金余额查询

电子现金余额查询命令允许终端直接读取卡中可脱机消费的余额。使用GET DATA命令取得电子现金余额。

该命令及响应的数据格式见表5和表6。

表5　电子现金余额查询 GET DATA 命令

字节	值	说明
CLA	“80”	
INS	“CA”	
P1	“9F”	“9F79”为电子现金余额标签。
P2	“79”	
L_c	不存在	
Data	不存在	
Le	“00”	

表6　电子现金余额查询响应

字节	值	说明
标签（T）	“9F79”	
长度（L）	“06”	6 字节长。
数据（V）	电子现金余额	以应用定义的货币表示。
SW1/SW2		状态信息，见 JR/T 0025.5—2018。

电子现金余额以应用定义的货币形式表示。

10.2　日志查询

卡片中存放的交易日志和圈存日志应能被终端以READ RECORD命令读取。

该命令的数据格式见表7和表8。

表7 READ RECORD 命令

字节	值	说明
CLA	“00”	
INS	“B2”	
P1	记录号	见 P1 和 P2 结构表。
P2	引用控制参数	
L_c	不存在	
Data	不存在	
Le	“00”	

READ RECORD命令中P1和P2参数域的取值见表8。

表8 P1 和 P2 结构表

字节	位	含义	值
P1	1～8	记录号	00：用于一次性获取卡内圈存日志的全部记录，并且返回的记录内容通过 MAC 确保记录完整性。 记录号：1 至应用支持的最大记录号（最小为 10）。实际大小定义于 FCI 中。
P2	8～4	短文件标识符 SFI	交易日志的推荐值为 0x0B。 圈存日志的推荐值为 0x0C。
	3	P1 为记录号	1
	2	未使用	0
	1	未使用	0

交易日志中各数据元的顺序，由交易日志格式（9F4F）定义。该格式的推荐值定义于JR/T 0025.5—2018，如表9，交易日志格式（9F4F）应通过Get Data命令获取。

表9 交易日志格式（9F4F）推荐值

标签	数据	长度（字节）
9A	交易日期	3
9F21	交易时间	3
9F02	授权金额	6
9F03	其他金额	6
9F1A	终端国家代码	2
5F2A	交易货币代码	2
9F4E	商户名称	20
9C	交易类型	1
9F36	应用交易计数器（ATC）	2

圈存日志中各数据元的顺序，由表10定义。记录圈存日志时，不应包括应用基本数据模版（标签‘70’），也不应记录数据元的标签和长度，应仅记录其值，圈存日志格式（DF4F）应通过Get Data命令获取。表10中序号为1至4的项是圈存日志中的固定内容，序号为5的项是圈存日志中的可变内容，其值可由发卡机构自定义，其值宜参照表11。

表10　圈存日志内容列表

序号	数据	长度（字节）
1	Put Data 命令的 P1 值（取值为 0x9F 或 0xDF）	1
2	Put Data 命令的 P2 值（取值为 0x79）	1
3	Put Data 修改前 9F79 或 DF79 的值	6
4	Put Data 修改后 9F79 或 DF79 的值	6
5	圈存日志格式（DF4F）中定义的数据元的值（见表 11）	可变
注：表10中的DF79的定义请见JR/T 0025.15—2018。		

表11　圈存日志格式（DF4F）推荐值

标签	数据	长度（字节）
9A	交易日期	3
9F21	交易时间	3
9F1A	终端国家代码	2
9F4E	商户名称	20
9F36	应用交易计数器（ATC）	2

最近的交易包含于记录 1 中，次近的包含于记录 2 中，依此类推。

如果终端试图读取一个空记录，卡返回错误（SW1 SW2=“6A83”）。以下情况可能出现空记录：

——日志中没有交易记录（如，新发卡）；

——P1 大于最大的记录号（最大的记录号指当前卡片交易明细记录中最大的记录条数）。

要读出交易日志中的完整内容，终端应从记录1开始，之后每次记录号加1重复执行READ RECORD命令。当卡响应SW1 SW2=“6A83”表示已读出了日志最后一项记录[2)]。

要一次性读取全部圈存日志，终端发送READ RECORD命令（P1=00），卡片响应的报文数据域见表12。

表12　P1=00 时读圈存日志响应的报文数据域

标签	数据	长度（字节）
--	应用交易计数器（ATC）[a]	2
--	后续日志记录数[b]	1
--	实际日志数据[c]	Var
--	日志完整性验证码	4
[a] 应用交易计数器（ATC）是卡片内当前的应用交易计数器的值。 [B] 后续日志数据记录数是后续的实际日志记录的条数。 [C] 实际的日志数据应从圈存日志文件，依次提取表13数据连接而成。		

表13　实际日志数据

标签	数据	长度（字节）
-	Put Data 命令的 P1 值（取值为 0x9F 或 0xDF）	1
-	Put Data 命令的 P2 值（取值为 0x79）	1
-	Put Data 修改前 9F79 或 DF79 的值	6
-	Put Data 修改后 9F79 或 DF79 的值	6

2)　日志的确切容量取决于发卡行的实现。

标签	数据	长度（字节）
-	交易日期	3
-	交易时间	3
-	应用交易计数器（ATC）	2

该数据最多返回最近10*22个字节的日志数据内容。当卡内圈存日志文件有多于10条记录时，仅取最新的10条记录；当卡内圈存日志文件记录不足10条时，取卡内实际存在的所有记录；当卡内圈存日志文件没有记录时，没有实际日志数据域，此时后续日志记录数为“00”。

日志完整性验证码是为了防止圈存日志信息从卡内取出后发生篡改，确保日志的完整性。其算法见JR/T 0025.5—2018附录C.2 MAC计算，其中JR/T 0025.5—2018附录C.2.4中数据块D由应用交易计数器（ATC）、后续日志记录数和实际日志数据按顺序连接而成。

10.3 取交易日志格式命令

为正确解释交易日志中包含的数据，终端需要知道其数据格式。该格式定义于文件控制信息FCI中。使用表14中各项命令读取交易日志格式。

表14 取交易日志格式 GET DATA 命令

字节	值	说明
CLA	“80”	
INS	“CA”	
P1	“9F”	“9F4F”为日志格式数据标签。
P2	“4F”	
L_c	不存在	
Data	不存在	
Le	“00”	

响应数据为交易日志，日志格式按照类似于DOL（数据对象列表）的方式编码。数据元格式见表9。

10.4 更新电子现金参数命令

卡片上的电子现金参数可通过JR/T 0025.5—2018中的PUT DATA命令进行更新。发卡行主机在授权响应中以脚本形式构造并发送该命令。可通过脚本命令更新的卡片电子现金参数有四个：电子现金余额、电子现金余额上限、电子现金单笔交易限额、电子现金重置阈值。使用表15和表16中的命令格式更新电子现金参数。

表15 更新电子现金余额 PUT DATA 命令

字节	值	说明
CLA	“04”	
INS	“DA”	
P1		P1 和 P2 为电子现金参数的标签。
P2		
L_c	“0A”	
Data	数值	电子现金参数的新值。
Le	“00”	

表16 电子现金参数 P1、P2 值

数据元名称	P1	P2
电子现金余额（EC Balance）	9F	79
电子现金余额上限（EC Balance Limit）	9F	77
电子现金单笔交易限额（EC Single Transaction Limit）	9F	78
电子现金重置阈值（EC Reset Threshold）	9F	6D

成功更新变量值的响应状态字为SW1 SW2=“9000”，其他可能出现的错误状态字定义按JR/T 0025.5—2018的规定。

11 电子现金简介

关于电子现金简介概述参见附录D。

附 录 A
（资料性附录）
卡片应用实例

本附录给出卡片正常生命周期中，电子现金余额和电子现金额度如何改变的实例。表A.1列举了各种事件。

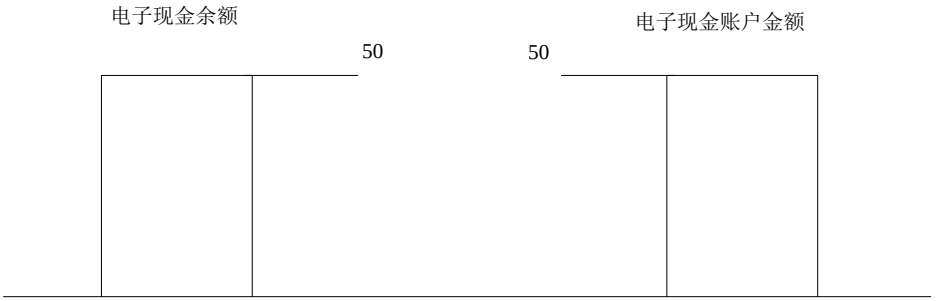
表A.1 卡片应用实例事件

序号	时间	事件	授权金额	说明
1	第 1 天	初始状态	50	发卡时初始电子现金余额为 50。
2	第 2 天	购买商品	5	
3	第 3 天	购买商品	10	
4	第 4 天	购买商品	15	
5	第 5 天	对第 2 天的交易进行清算	5	
6	第 6 天	购买商品	7	
7	第 7 天	对第 4 天的交易进行清算	15	
8	第 8 天	对第 3 天的交易进行清算	10	

图A.1-图A.8采用上表所描述的事件，展示了在卡的典型生命周期内，卡电子现金余额与电子现金额度如何交互改变。

事件1——初始化状态

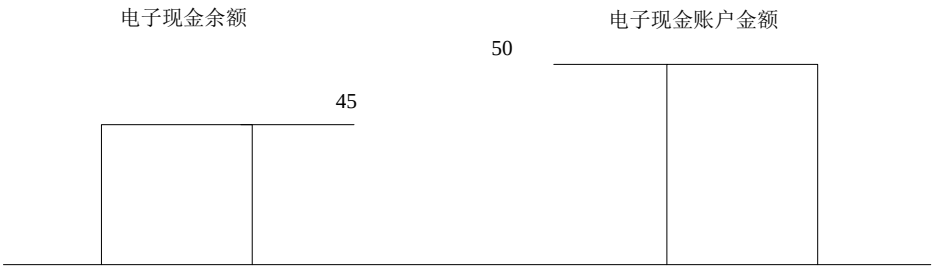
初始化状态见图A.1所示。



图A.1

事件2——购买商品5元

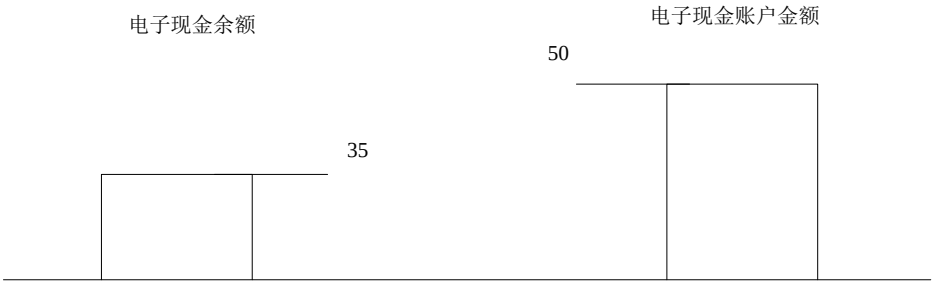
交易被脱机批准，卡电子现金余额被更新。由于还没清算，电子现金账户仍然未变。见图A.2所示。



图A.2

事件3——购买商品10元

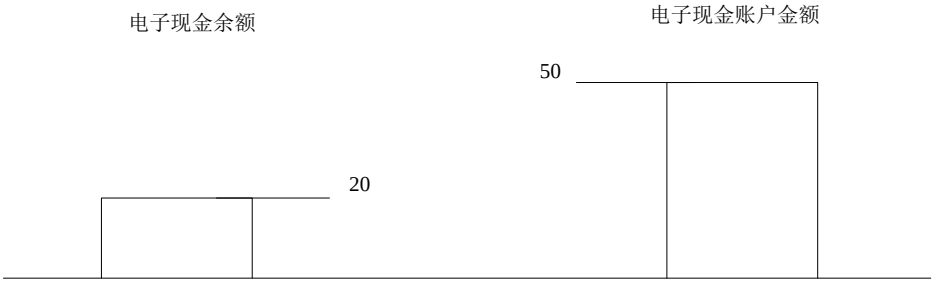
交易被脱机批准，卡电子现金余额被更新。由于还没清算，电子现金账户仍然未变。见图A.3所示。



图A.3

事件4——购买商品15元

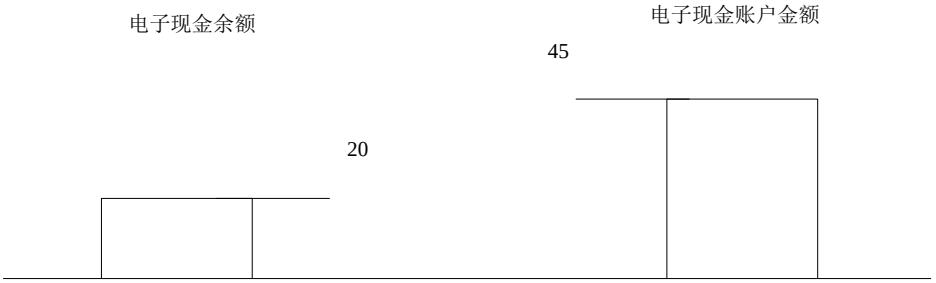
交易被脱机批准，卡电子现金余额被更新。由于还没清算，电子现金账户仍然未变。见图A.4所示。



图A.4

事件5——将第2天的5元购买交易清算

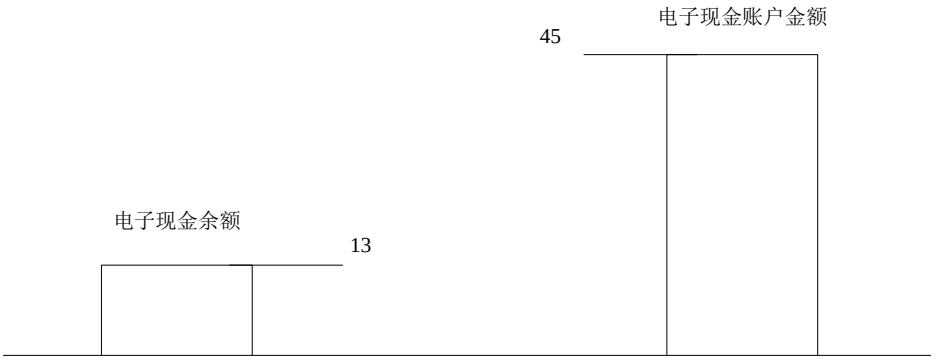
清算报文用于更新电子现金账户金额。清算后状态见图A.5所示。



图A.5

事件6——购买商品7元

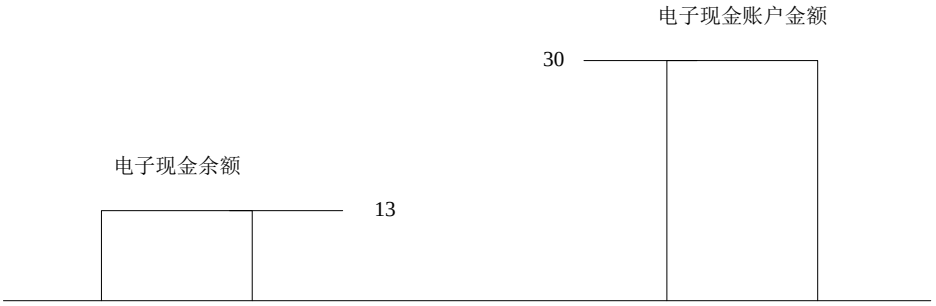
交易被脱机批准，卡电子现金余额被更新。由于还没清算，电子现金账户仍然未变。见图A.6所示。



图A.6

事件7——将第4天的15元购买交易清算

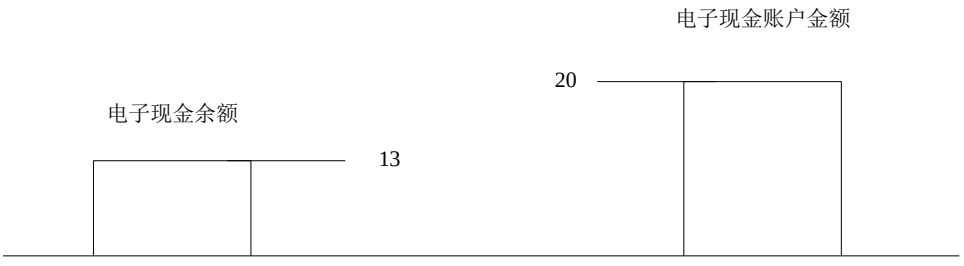
清算后状态见图A.7所示。



图A.7

事件8——将第3天的10元购买交易清算

清算后状态见图A.8所示。



图A.8

附 录 B
（资料性附录）
电子现金交易的要求及实现

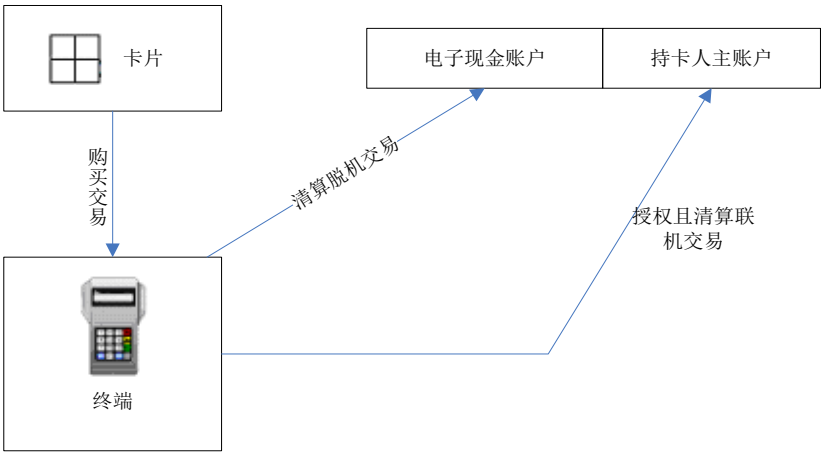
B.1 支付交易

B.1.1 功能概述

使用具有电子现金功能的金融IC卡支付与使用标准借记/贷记卡的支付行为并无区别。

关于交易期间卡与终端间命令流的描述见JR/T 0025.5—2018。

金融IC卡执行电子现金脱机交易，是针对卡电子现金余额进行的。之后由发卡行针对电子现金账户金额进行交易清算。若支付交易未被脱机批准，则由发卡行联机授权。发卡行通常针对持卡人主账户进行授权和清算。电子现金支付示例如图B.1所示。



图B.1 具有电子现金功能的金融 IC 卡的支付交易

B.1.2 功能描述

当持卡人将具有电子现金功能的金融IC卡插入POS终端时，按照JR/T 0025—2018所描述的，终端选择卡应用。与JR/T 0025—2018一致，终端也执行一系列操作，包括检查卡是否真实（卡片认证方法（CAM）），以及持卡人是否真实（持卡人验证方法（CVM））。

脱机交易：

终端将交易相关的数据，以及其他同交易相关的环境数据传送至金融IC卡，卡片则将其自己的交易相关数据提供给终端。

金融IC卡使用电子现金余额以及授权金额，来判断交易是否可脱机授权。

只有交易以应用货币（由发卡行在个人化时向卡应用指定）进行时，方可脱机授权。以其他货币进行的交易将被迫联机进行。

卡将测试如下信息：

——当前交易期间收集的交易状态信息；

——上次交易保留的状态信息。

测试结果帮助卡决定后续做法：

——脱机拒绝交易；

——对交易脱机授权批准；

——将交易发送至发卡行联机授权。

如果交易被脱机批准，卡从其电子现金余额中减去本次授权金额，并生成交易证书（TC）密文。终端将此密文及相关的交易数据发送给收单行，收单行可能将此包含在他向发卡行提供的清算提交当中。此交易证书（TC）为发卡行提供交易已发生的证据，并用于支持商户的支付要求。

联机交易：

如果由于某种原因，交易未被脱机批准，卡将生成授权请求密文（ARQC）。此密文以及相关的交易数据，被递交给发卡行用于联机授权处理。

除其他芯片相关数据元外，卡还将当前电子现金余额发送给发卡行。

当发卡行接收到ARQC时，分析芯片数据，以识别联机请求的原因。

请求交易联机授权的原因包括：

——卡电子现金余额不足以支持本次交易。如果此情况发生，则发卡行可采取以下一种措施：

- 由于金额不足拒绝交易；
- 从持卡人主账户中转移更多金额至电子现金账户金额中，假定（发卡行与持卡人）已达成一份自动圈存协议。

——交易货币与卡应用货币不匹配。如果此情况发生，则发卡行可能针对持卡人主账户余额进行交易授权。这类交易与标准的借/贷记交易以相同方式处理。

无论发卡行对本次交易给出何种响应，均可向卡发送指令以调整其电子现金余额。对电子现金余额的调整可能具有如下形式：

——增加（从持卡人主账户转移至电子现金账户金额）；

——减少（授权金额）。

金融IC卡使用发卡行的指令作最终的授权决定。如果卡批准交易，则商户继续发货或提供其他服务。如果卡拒绝交易（生成应用认证密文AAC），则终端终止交易。

如果交易已授权，则商户应在日销售结算时，将交易证书TC发送至收单行，作为交易已完成的证据。收单行需保存TC密文以备为将来可能出现的争端提供证据。

B.1.3 异常处理

源自借记/贷记应用的交易异常处理，对于具有电子现金功能的金融IC卡的处理和标准借记/贷记卡是相同的。异常处理是一个可能导致电子现金账户金额与卡电子现金余额产生差异的过程。

最常见的异常情况有：

——交易取消：在卡电子现金余额已被调整后，交易被持卡人、商户或者终端（由于技术故障）取消；

——退款：商户将交易额退还（持卡人）；

——争议：持卡人对交易产生争议。

后续将详细描述各种异常情况。

交易取消：

交易可能在卡与终端已完成期间的交互后被取消。取消的原因可能包括：

——终端故障；

——发货、提供服务或现金期间发现失误。

当由于以上原因交易被取消时，若交易被联机授权，终端将创建冲正报文发送给发卡行，冲正报文以磁条卡的方式处理（即存入到持卡人主账户，而不反映至卡余额或电子现金账户金额），终端不能将交易金额重新存入卡片电子现金余额[3)]；如果交易被脱机批准，则可采用物理货币的方式退还给持卡人。

退款：

当商户将交易额退还持卡人时，既可采用物理货币形式，也可在相应产品规则和政策允许的前提下，将金额存入卡账户。现金返还不会给具有电子现金功能的金融IC卡带来问题，因为交易额已从卡电子现金余额中支出。当采用退款交易时，这种退款方式的结果是持卡人主账户有金额存入，却不能自动反映至卡余额或者电子现金账户金额。

取消：

和退款类似，取消有时可导致主账户、电子现金账户金额和卡脱机账户间的差异。

争议：

电子现金交易中出现的持卡人争议和标准金融IC卡交易中出现的持卡人争议，在处理上并无区别。

然而，在持卡人对电子现金余额值产生争议时（如退款或取消后），问题可能出现。发卡行应知道这些争议存在的可能，并实现相应的措施予以调查（如检查卡的交易日志）。

同步失败：

可能会出现卡的电子现金余额与发卡行主机中的电子现金账户金额不相等的情形。一般来说，这是由于有交易脱机进行且未清算所致。

发卡行可利用脚本来修改卡片中的电子现金余额。

B.1.4 要求与约束

电子现金的一个主要业务需求是，提供低风险的脱机交易。为实现此需求，需考虑以下功能要求：

——终端要求；

——收单行处理要求；

——卡要求；

——发卡行处理要求。

终端要求：

关于交易期间卡片与终端之间命令流的详细描述，按JR/T 0025.4—2018的规定执行。

具有电子现金功能的金融IC卡应与终端交互，并按照JR/T 0025—2018中借记/贷记应用相关要求来处理交易。收单行应按照本部分来实现其终端的设置。收单行应实现以下功能以确保脱机能力：

——脱机 CAM 支持；

——脱机 PIN 支持（可选）；

——终端最低限额。

为保持电子现金余额的完整性，具有电子现金功能的金融IC卡应支持动态数据认证（DDA）。因此接受具有电子现金功能的金融IC卡的终端应进行动态数据认证（DDA）。

收单行处理要求：

收单行系统应按JR/T 0025—2018的要求，将芯片数据传送给发卡行。包括：

——在联机授权请求与响应中传送芯片数据；

——保存芯片数据以备将来可能出现的争议。

收单行可能在清算记录过程中传送芯片数据，但不强制此做法。传送芯片数据可帮助发卡行管理其联机账户。

---

3) 发卡行应确保（通过对持卡人细致的培训），使持卡人不应因交易被撤销且卡余额未更新而导致的余额差异情况产生误解。

卡要求：

具有电子现金功能的金融IC卡应符合JR/T 0025—2018中关于借记/贷记应用的要求。

发卡行处理要求：

一般来说，电子现金交易在脱机状态下进行，发卡行针对电子现金账户对这些交易进行清算。联机交易（无论使用金融IC卡或磁条卡）则一般针对主账户进行授权和清算。

B.2 ATM交易

B.2.1 功能概述

发卡行以与其他ATM交易相同的方式，处理具有电子现金功能的金融IC卡（带借记/贷记功能）的ATM现金支取。ATM现金支取总是由发卡行主机针对持卡人主账户进行联机授权的。

B.2.2 功能描述

如JR/T 0025—2018中所描述，当持卡人将具有电子现金功能的金融IC卡插入ATM终端时，终端选择卡应用。

终端传递交易及其他相关的数据给卡，卡提供其交易相关的数据给终端。此数据交换使交易处理继续进行。

ATM交易总是需要请求由发卡行进行的联机授权。这种做法可让发卡行将ATM现金支取的脱机风险管理降为最低。ATM要求卡生成授权请求密文（ARQC），并将此ARQC密文和交易支持数据，发送至发卡行以进行授权处理。

发卡行针对持卡人主账户余额进行交易授权。金额从主账户中支出（电子现金余额不受影响）。发卡行的响应通知卡不用调整其电子现金余额。

当接收到发卡行的响应时，金融IC卡使用包含于该响应中的指令做出其最终决断。卡可进行以下一种选择：

——批准交易，ATM 提供现金（和凭证，如果要求的话）；

——拒绝交易，ATM 告知持卡人交易被拒绝的原因（如果提供了相关可读信息的话），并终止交易。

如果交易被授权，卡将产生交易证书（TC）。收单行应保存此交易证书，以备发生争议时供发卡行查询。

B.2.3 异常处理

没有与具有电子现金功能的金融IC卡ATM现金支取相关的异常情况。

B.2.4 要求与约束

终端要求：

处理电子现金交易，对ATM终端没有特别要求。

收单行处理要求：

处理电子现金ATM交易，对收单行系统没有特别要求。

卡要求：

处理电子现金ATM交易，对卡没有特别要求。

发卡行处理要求：

电子现金ATM支取，对发卡行系统处理没有特别要求。

B.3 圈存交易

B.3.1 功能概述

为使持卡人能继续使用具有电子现金功能的金融IC卡进行脱机交易，在初始金额已消费完后，应能够转入金额以增加电子现金账户金额。实现该目的的全过程称为“圈存”。圈存实际包括两步：

——金额预授权：此为增加电子现金账户金额；

——卡片充值：将余额增加反映至卡电子现金余额。

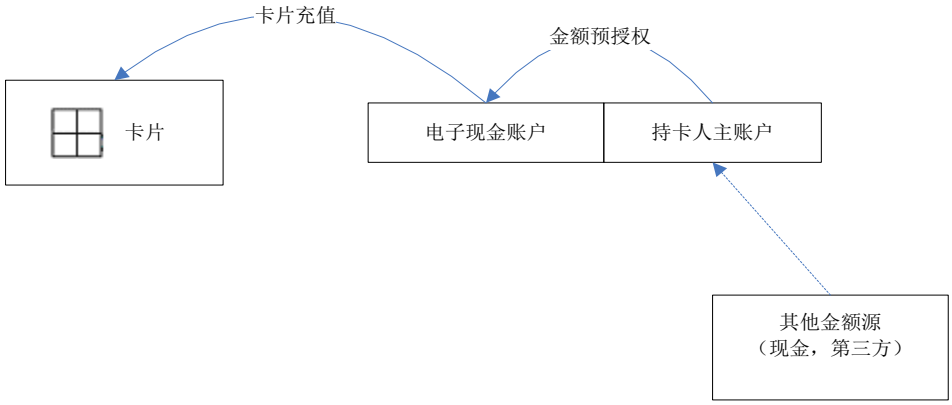
圈存的金额可以有以下几个来源，包括：

——持卡人的主账户；

——现金支付，如在银行柜面的现金支付；

——第三方，如父母将金额转入其子女账户等。

电子现金圈存示例如图 B.2 所示。



图B.2 电子现金圈存功能

B.3.2 功能描述

发卡行可使用以下选项来增加电子现金余额：

——持卡人发起的金额转入（手动），从持卡人主账户至电子现金账户金额；

——发卡行发起的金额转入（自动），从持卡人主账户至电子现金账户金额。假定发卡行与持卡人之间已签订相关协议，使得当电子现金账户金额低于某值（电子现金重置阈值）时，或者在某特定交易但卡中电子现金余额不足时，能够自动完成金额转入。此处有一前提假设，即电子现金账户金额的增加会尽可能快地反映至卡电子现金余额。卡片充值处理根据圈存处理发起方的不同而有所区别；

——持卡人发起的手动圈存：处理立即进行，因为卡应与发卡行联机通信以执行该过程，主机因此可发送脚本去执行卡充值操作，作为本次联机通信的一部分；

——发卡行发起的自动圈存：处理被延迟，直到发卡行能够与卡联机交换信息（如，当下次交易被提交联机授权时）。

B.3.3 手动圈存

B.3.3.1 持卡人发起的从主账户进行圈存

允许持卡人自己监视电子现金余额，并选择何时对卡片进行充值。

在提供圈存设备的地方，持卡人可使用这些设备来增加具有电子现金功能的金融IC卡的电子现金余额。发卡行应确保持卡人能够识别这些终端，如通过采用特定的记号标识这些终端，或者通过印发产品宣传单等方式。

具体实现由发卡行自定义，表B.1内容可供参考：

表B.1　手动圈存相关操作

步骤	行为
1	持卡人将卡片插入终端（终端识别出此为一张具有电子现金功能的金融 IC 卡）[a]。
2	终端向持卡人提供服务列表，其中包括“对卡圈存”。
3	持卡人选择圈存功能[b]。
4	持卡人选择充值金额。
5	终端开始进行标准借记/贷记交易[c]。
6	将联机授权请求发给主机系统，一起发送的还有发卡行自定义指示符，告诉主机持卡人选择了何种圈存功能。
7	发卡行主机对金额转移进行校验，并进行联机处理的常规检查[d]。
8	主机系统处理联机交易，并构造授权响应，其中包括响应密文，以使卡能验证该响应的合法性。
9	主机系统构造更新电子现金参数脚本命令，该命令数据中包含新的电子现金余额值。
10	将授权响应和脚本一同发回给卡，以更新其电子现金余额。
11	终端宜将确认报文送回主机，表明圈存是否成功。
[a] 终端可通过读取 IC 卡中电子现金数据项（包含电子现金余额（9F79）、电子现金余额上限（9F77）、电子现金单笔交易限额（9F78）等），通过以下两种方式判断卡片是否支持电子现金应用： ——电子现金余额大于 0； ——电子现金余额上限大于 0，并且电子现金单笔交易限额也大于 0。 [b] 如果有不只一个账户可用于圈存的金额源，系统会提供一个账户列表，持卡人可选择从哪个账户中借记。 [c] 借记/贷记处理包括提示持卡人输入 PIN 并执行脱机 CAM。终端要求卡生成 ARQC 并将交易送至联机进行。可将卡与终端之间交互的授权金额设为充值金额，以作为充值明细查询时的参考 [d] 如，发卡行可检查卡片是否已报挂失。	

当持卡人选择圈存功能时，终端将提示输入圈存额（取决于具体的实现，终端可能首先与发卡行主机系统进行交互，检查可供圈存的额度，并告知持卡人）。

借记/贷记处理完成后（即对第2个GENERATE AC命令响应，成功生成了AC，发卡行已发送了脚本命令），发卡行可定义一种私有机制，以确定更新是否成功。圈存一般在ATM或银行柜面终端上进行，在主机确定圈存成功完成前，这些终端应确保不吐出卡片。

要将交易送至联机进行，终端要求卡生成一个授权请求密文（ARQC）并发送至主机系统。当请求ARQC时，终端应包含来自卡数据对象列表（CDOL）数据元“CDOL1”的卡数据。此外终端还应提供所有在消费或取现交易中终端所需提供的相关交易数据。此信息包括授权金额与货币形式（此处指圈存额和货币形式）。

终端产生联机授权请求时，应包含一个用于标记本次交易为圈存请求的标识。用于标识圈存请求的方法，由发卡行自定义。

当发卡行收到ARQC后，将进行如下检查：

——检查来自具有电子现金功能的金融 IC 卡请求的合法性；

——检查包含于请求中的 ARQC 密文和金融 IC 卡数据；

——检查联机 PIN（如果包含的话）。

如果上述检查均通过，则发卡行将请求的金额从持卡人主账户划入电子现金账户。

发卡行给终端的响应表明请求是否通过。如果请求未通过，则响应中说明未通过的原因。除了给出响应外，发卡行还返回脚本命令，让金融IC卡调整其电子现金余额，以反映新的电子现金账户金额值。

接收到发卡行的响应后，金融IC卡根据里面的指示产生最终的交易决断，方式与支付交易或ATM现金支取相同。终端传递脚本命令给卡，以调整其电子现金余额。读取卡中新的电子现金余额值并向持卡人显示后，整个圈存过程完成。

持卡人发起的圈存总是联机进行，因为发卡行主机应检查是否有足够的金额可供圈存。执行联机检查后，才允许主机系统进行卡充值操作。

B.3.3.2 持卡人发起的现金圈存（可选）

发卡行允许持卡人通过现金支付形式对其具有电子现金功能的金融IC卡进行圈存。一般需要银行业务员确认现金额，并在银行柜面终端上完成。

若支付被接受，银行业务员将金额输入持卡人电子现金账户。对于现金支付来说，金额被立即划至账户中。持卡人将具有电子现金功能的金融IC卡插入柜台终端，以与其他终端类型相同的方式，开始圈存交易。

柜台终端与主机系统间的交互方法，可由发卡行自定义。对于其他形式的圈存终端，例如委托特定的商户或具有现金存款功能的ATM来说，与上述方法类似。

B.3.4 自动圈存

发卡行可与持卡人建立一份协议，以允许从持卡人主账户或其持有的其他账户中实现自动圈存。以下情况可激发发卡行发起自动圈存：

——将电子现金余额值与电子现金重置阈值比较。如持卡人要求，每当电子现金余额低于电子现金重置阈值时，进行自动圈存；

——联机交易请求，由于卡中电子现金余额太低，未批准脱机交易而转入联机交易。

自动圈存的实现方法由发卡行自定义，表B.2可供参考：

表B.2 自动圈存相关操作

步骤	行为
1	主机收到授权请求（如授权金额超出卡电子现金余额）。
2	主机系统识别出： —— 卡请求联机授权的原因； —— 卡电子现金余额少于当前授权金额。
3	主机系统开始从主账户进行金额转移（如果发卡行与持卡人间已取得关于自动圈存协议的话）[a]。
4	主机系统进行其私有处理，从主账户进行金额转移，之后使用脚本去更新卡电子现金余额。
5	授权系统发送授权响应，表明交易已被授权。其中包括响应密文，允许卡对发卡行进行认证。
6	将响应密文和脚本一起发回给卡，以重设电子现金余额。
[a] 可以是预先协商的一个值。如，持卡人同意当电子现金余额用尽时，转移 50 元，或者将卡加至某值（如加至使电子现金余额为 50 元）。	

若是卡电子现金余额不足以对交易脱机授权，则接下来的处理方式取决于发卡行对卡授权请求的响应。可选的处理方式有：

——如果由于除金额不足外的任何原因，导致不能进行脱机批准的，则发卡行拒绝本次交易，不作任何金额转移；

——如果仅由于授权金额的原因，导致不能进行脱机批准的，且授权金额小于或等于电子现金余额和主账户余额的总和，则发卡行可进行如下做法：

- 将协议充值金额转移至电子现金账户；

- 对金融 IC 卡生成授权响应；
- 生成脚本命令调整卡电子现金余额。

——如果仅由于授权金额的原因，联机授权被拒绝，且授权金额大于电子现金余额及主账户余额的总和，则发卡行将对金融 IC 卡产生拒绝授权报文（原因是“金额不足”）。

接收到发卡行的响应后，卡利用其中的指令生成最终的交易判决。之后终端将脚本命令发送至卡，更新电子现金余额，整个圈存过程完成。

在本次或下次联机交易时，主机系统应检查卡中新的电子现金余额是否准确反映圈存结果。

B.3.5 异常处理

具有电子现金功能的金融IC卡的借记/贷记异常处理，与标准借记/贷记卡的异常处理基本相同，除以下情况外：

——发出圈存请求但无可用金额：

当发出圈存请求，但持卡人主账户中金额不足时，不进行圈存处理，除非发卡行允许从主账户透支；若持卡人中断圈存操作，则交易被拒绝，终端向持卡人表明圈存被拒绝的原因。

——更新卡电子现金余额期间，交易被持卡人或终端（由于技术故障）取消：

如果终端实现了其私有的圈存功能，发卡行将接收到圈存交易的成功或失败（即，被送至更新卡电子现金余额的脚本的成功或失败）确认。该确认可让发卡行正确调整电子现金账户金额。若终端不能发送确认，则发卡行无法收到关于脚本处理的结果确认，主机系统应通过其他方式检查该结果。

对于发卡行发起的圈存交易，圈存交易的处理状态以与其他脚本命令相同的方式报告。

——持卡人对交易产生争议：

若持卡人对圈存处理的结果产生争议，则由持卡人与发卡行签订的协议条款裁定。

B.3.6 要求与约束

终端要求：

支持持卡人发起圈存的终端应实现与持卡人的对话功能，以及某种形式的圈存交易标识以支持圈存功能。该类终端还应支持JR/T 0025.6—2018的7.12中定义的发卡行脚本处理。

发卡行需要了解在POS终端上进行圈存的某些潜在问题，如持卡人在电子现金余额被更新前拔出卡片。为避免此类问题，发卡行应将发卡行发起的圈存严格限制于ATM或柜台终端上进行。

收单行处理要求：

若支持发卡行发起的圈存，终端和收单行应支持以发卡行完全迁移模式与发卡行的联机通信。

卡片要求：

处理电子现金圈存交易对卡片没有特别要求。

发卡行处理要求：

发卡行脚本处理系统应能够对未执行的脚本进行处理，该类脚本在发卡行发起的圈存处理中经常遇到。

为避免对可疑卡片进行圈存，发卡行应将圈存功能与授权处理关联起来。

B.4 圈提交易

B.4.1 功能概述

如果持卡人或发卡行决定取消电子现金功能（如持卡人或发卡行想销卡），则需将卡片电子现金余额中的金额圈提给持卡人。

圈提与圈存刚好相反，包括以下两步：

——清空卡余额；

——返还持卡人。

B.4.2 功能描述

清空卡余额：

首先，发卡行应将用于脱机消费的电子现金余额设为“0”。实际的实现机制由发卡行私定，以下可供参考：

——持卡人将卡片插入发卡行自己的具有联机功能的终端(ATM 或银行柜面终端)，并选择“圈提”；

——终端执行余额查询，以查看卡片电子现金余额值；

——终端进行空交易，并从卡片请求 ARQC；

——终端将报文发送至主机系统，指示余额将被清空；

——主机记录电子现金余额值并检查是否有未清算交易；

——主机以“拒绝”响应终端，并发送脚本命令将电子现金余额设置为“0”；

——终端向卡请求 AAC，并发送 ARPC 响应码；

——卡设置电子现金余额为“0”，并以 AAC 回复。

返还持卡人：

通过上述过程圈提的金额没有任何需等待清算的交易，因此可将金额立即返还给持卡人。然而终端需要向主机系统确认，卡片已正确完成命令，此时发卡行可将金额返还给持卡人。

发卡行可在此处检查卡片电子现金余额与电子现金账户金额是否相等，存在两种可能结果：

——如果相等，则没有明显需要等待清算的交易，不需进一步的操作；

——若电子现金余额小于电子现金账户金额，表示卡进行了未被清算的脱机交易，需要执行如下另外两个步骤：

- 发卡行需等到清算完成，或者从应用交易计数器的值确认，在圈提电子现金账户金额中剩余的金额前没有明显的未处理交易；
- 发卡行将金额返还给持卡人。返还额一般为从卡中圈提的额度。

鉴于发卡行实现电子现金账户的方式不同，圈提可能出现如下结果：

——将电子现金账户金额中的金额划入持卡人主账户；

——现金支付给持卡人。

B.4.3 异常处理

没有与圈提交易相关的特殊异常情况。

B.4.4 要求与约束

终端要求：

处理圈提交易，应在具有联机功能的终端（ATM或银行柜面终端）上进行。

收单行处理要求：

处理圈提交易，对收单行系统没有特别要求。

卡要求：

处理圈提交易，对卡没有特别要求。

发卡行处理要求：

处理圈提交易，对发卡行系统处理没有特别要求。

B.5 修改电子现金余额上限交易

B.5.1 功能概述

可给具有电子现金功能的金融IC卡的持卡人提供更高的脱机消费能力。

修改电子现金余额上限应在金融终端上联机进行，且应提交个人识别码（PIN）。

修改电子现金余额上限的具体业务做法和要求不在本部分中规定。

B.5.2 功能描述

是否采用此功能以及重新设定的值由发卡行决定。

采用此交易，在联机处理期间，发卡行可简单地发送一个脚本来设置一个新的上限值。

该新的“电子现金余额上限”值代表了在电子现金应用中，持卡人实际可脱机消费的最大累积额度。一旦脱机交易总额超出该值，亦即授权金额超过了电子现金余额，则所有交易应通过联机授权。此上限值越大，实际能脱机消费的额度也就越大。

该值的设定由发卡行根据持卡人的具体情况而定。

B.5.3 异常处理

没有与修改电子现金余额上限功能相关的特殊异常情况。

B.5.4 要求与约束

终端要求：

处理修改电子现金余额上限交易，应严格限制于ATM或银行柜面终端上进行。

收单行处理要求：

处理修改电子现金余额上限交易，对收单行系统没有特别要求。

卡要求：

处理修改电子现金余额上限交易，对卡没有特别要求。

发卡行处理要求：

修改电子现金余额上限，对发卡行系统处理没有特别要求。

B.6 查询日志交易

B.6.1 功能概述

符合JR/T 0025—2018的卡应用，保存了卡最近进行的芯片交易内部日志。

对于每次交易，卡片在其交易日志中可保存以下信息：

——交易日期；

——交易时间；

——授权金额；

——其他金额；

——终端国家代码；

——交易货币代码；

——商户名称；

——交易类型；

——应用交易计数器（ATC）。

发卡行通过交易日志查询功能，向持卡人提供卡片最近的行为信息。

欲向持卡人提供交易日志服务的发卡行，应在其控制下的终端上实现交易日志查询功能，或与发行了具有电子现金功能的金融IC卡地区的收单行协商实现该功能。

B.6.2 功能描述

要读取交易日志，终端仅需选择支付应用，并向卡发送读交易日志命令，见本部分10.3。

终端不可将状态信息或技术信息向持卡人透露。宜将交易信息严格限定为以下内容：

——日期；

——货币；

——金额。

一旦终端将这些信息向持卡人展示后，交易即可终止，无需与卡进一步的交互。

B.6.3 异常处理

没有与电子现金交易日志查询功能相关的特殊异常情况。

终端需要处理以下可能出现的异常情况：

——插入的卡片不支持交易日志；

——交易日志中无条目项。

B.6.4 要求与约束

终端要求：

交易日志查询的详细资料定义遵照JR/T 0025.6—2018中B.2的规定。关于终端需求的技术细节，见本部分10.2。

收单行处理要求：

如果发卡行与收单行协商提供该功能，则收单行终端可按JR/T 0025.6—2018中B.2中的规定提供查询日志功能。

卡片要求：

要使用交易日志查询功能，需在卡片个人化时激活该特性。

发卡行处理要求：

交易日志查询功能一般脱机情况下执行，对发卡行系统没有影响。如果发卡行将交易日志查询功能扩展为允许联机更新，则按照一般联机规则实现。

B.7 查询余额交易

B.7.1 功能概述

电子现金余额查询功能提供返回卡片中的电子现金余额。电子现金余额为可供脱机消费的剩余金额。

欲向持卡人提供此服务的发卡行应在其直属的终端上，或者诸如手持读卡器之类的其他设备上，实现电子现金余额查询功能，或者同具有电子现金功能的金融IC卡发行地的收单行协商实现该功能。

若发卡行仅在部分终端上提供该服务，则应采取某种方式让持卡人识别出哪些终端提供该服务（如采用某特定标记）。

B.7.2 功能描述

为读取卡电子现金余额，终端需选择支付应用，并向卡发送GET DATA命令。

终端接收到来自卡的电子现金余额，作相应格式化后向持卡人显示。他让持卡人知道目前卡中存有多少可供脱机消费的余额。

卡片电子现金余额以应用货币形式向持卡人显示。

发卡行自己的终端，如ATM或银行柜面终端等，一般均应支持电子现金余额查询。此外，一些小巧廉价的设备也提供该功能。实现电子现金方案的发卡行可以在发卡时便将这种余额读卡器一同提供给持卡人。

一旦终端已将电子现金余额向持卡人显示，便终止交易并关闭接口，不再与卡发生进一步的交互。

B.7.3 异常处理

没有特殊的异常情况与电子现金余额查询功能有关。但终端需要能够对插入但不支持余额查询的卡进行管理。

B.7.4 要求与约束

终端要求：

电子现金余额查询功能由电子现金产品自定义，需在标准借记/贷记终端（标准借记/贷记终端仅支持借记/贷记金融IC卡）上作单独实现。关于终端需求的详细技术细节，见本部分10.1。

收单行处理要求：

如果发卡行与收单行协商提供该功能，则其实现方式见本部分10.1。

卡片要求：

实现电子现金余额查询功能对卡片没有特殊要求。

发卡行处理要求：

电子现金余额查询功能一般脱机执行，对发卡行系统并无影响。若发卡行将该功能扩展为允许联机更新，则按照标准借记/贷记规则实现。

附 录 C
（资料性附录）
电子现金余额及日志读卡器功能要求

C.1 概述

C.1.1 要求概述

电子现金要求分成两大类：
——业务要求；
——安全性要求。
电子现金余额通过以下方法符合这些要求：
——增强持卡人功能选项；
——增加成员银行在脱机交易中管理风险的灵活性。
持卡人可使用一个小巧且廉价的个人设备来查看卡片的电子现金余额，或者也可查看卡片上的交易日志、圈存日志，这样的个人设备将有助于电子现金方案满足这些要求[4)]。

C.1.2 业务要求

个人设备（读卡器）应满足以下业务要求：
——支持电子现金余额的显示；
——支持交易日志条目的显示；
——支持圈存日志条目的显示；
——读卡器应价廉、自带电源，以及正常使用寿命在五年以上；
——读卡器可提供此处所提及之外的一些特性。
以下个人设备类型应支持表C.1里所列的功能。

表C.1 个人设备应支持功能

设备类型	功能		
	余额显示	交易日志的显示	圈存日志的显示
余额读卡器	M	O	O
日志读卡器	M	M	M

（其中：M—必备，O—可选）

C.1.3 安全要求

个人设备（读卡器）的安全要求是：
——余额、货币、交易日志显示的值应如实地反映卡中的数据；
——如果设备允许软件升级，那么应启用一些机制来保证其原始性和完整性，且在安装之前要确保对该型号的更新经过核准；
——卡片移除后，读卡器不应保留或者显示与卡相关的任何信息。

4) 该个人设备的特性并非专门用于电子现金，因为他们源自 JR/T 0025—2018，因此这样的设备也可使用于电子现金之外的其他应用。

C.2 功能概述

C.2.1 电子现金余额

从卡中取得电子现金余额方式，通常的方法是用GET DATA命令来读取余额。

C.2.2 用GET DATA命令取得电子现金余额

电子现金余额通过以下操作取得：

a) 卡上电；

b) 选择应用；

c) 用 GET DATA 命令读取电子现金余额。

另外，读卡器应从卡中取得货币代码，然后用查询表将其转换成文字格式。

C.2.3 显示交易日志

显示交易日志的步骤见表C.2。

表C.2 交易日志的显示步骤

步骤	行为
1	读卡器查看交易日志是否存在。
2	读卡器从卡中取得一系列表示日志格式和货币形式的标签。
3	读卡器用一系列 READ RECORD 命令从卡中读取日志。
4	数据由读卡器向持卡人显示。

应通过滚读方式读取所有的条目。该特定方法由发卡行自定，此处不作详细规定。

C.2.4 显示圈存日志

显示圈存日志的步骤与显示交易日志的步骤相同，见C.2.3的规定。

C.3 功能要求

C.3.1 电子现金余额

C.3.1.1 获取电子现金余额

表C.3列出了应在读卡器中定义的标签，以实现获取电子现金余额操作。

表C.3 获取电子现金余额过程的终端预定义标签

标签	类型	描述
9F79	B	电子现金余额
9F51	N	应用货币代码

为执行“读取电子现金余额”操作，读卡器执行以下动作：

a) 读卡器选择卡片应用。如果卡片应用的返回代码不是“成功”则读卡器终止“获取电子现金余额”过程，并产生“卡未被接受”的返回代码；

b) 然后读卡器通过 GET DATA 命令取得卡电子现金余额，GET DATA 命令定义见表 C.4；

表C.4 读取电子现金余额的GET DATA命令

代码	数值
CLA	80
INS	CA
P1	9F
P2	79
LE	00

c) 如果命令的返回状态字不是“9000”，则读卡器终止“获取电子现金余额”过程，并产生“卡未被接受”的返回代码；

d) 读卡器通过校验标签“9F79”来核实卡已经返回了电子现金余额。如果卡还没返回电子现金余额，则读卡器终止“获取电子现金余额”过程，并产生“卡未被接受”的返回代码。

C.3.1.2 显示电子现金余额

显示数据并无建议方法，因为他严格取决于显示特性的能力。以下建议只作指导：

——余额应显示为三字符的货币代码加上余额，并按照小数点位数进行格式化；

——如果由于显示大小所限，货币（形式）与余额值不能同步显示，则应先显示余额值，稍作延迟后再显示货币（形式），之后便在两者之间切换。

如果显示字符集不支持货币代码需要的字符显示集，则货币代码应以三个空格代替。

C.3.2 交易日志

C.3.2.1 读取交易日志

读卡器“读取交易日志”过程在交易日志查询时从卡片读取交易日志。

表C.5列出了为实现读取交易日志过程，终端应定义的标签。

表C.5 读取交易日志的终端（定义）标签

标签	类型	描述
84	B	DF名称
9F4F	B	交易日志格式
9F51	N	应用货币代码

读取交易日志过程返回以下输出参数：

——表示交易日志中条目数的整数值（n）；

——返回的代码；

——包含交易日志条目的二进制字符串。

交易日志组织为记录列表形式，其中第1个记录包含写进文件的最后一条（交易）记录。假定每条记录的长度为M，表C.6描述了交易日志是如何组织的。

表C.6 交易日志的组织形式

字节	交易日志
0	交易日志的最后一个条目
M	交易日志的倒数第2个条目
2M	交易日志的倒数第3个条目

…	…

表C.7描述了每个交易日志条目的格式。

表C.7　交易日志条目的格式

字节	数据元
3	交易日期
3	交易时间
6	授权金额
6	其他金额
2	终端国家代码
2	交易货币代码
20	商户名称
1	交易类型
2	应用交易计数器（ATC）

读取交易日志的过程如下：

a) 读卡器选取卡应用程序。如果卡应用程序的返回代码不是“成功”，则读卡器停止交易日志的读取，并产生“卡未被接受”的返回代码，否则读卡器从 SELECT 命令中获取的 FCI 数据中获取交易日志入口，以判断卡片是否支持交易日志，以及可能包含的最大记录数；

b) 读卡器发出 GET DATA 命令取得交易日志格式（9F4F）。表 C.8 描述了可使用的命令；

表C.8　用于取得交易日志格式的命令的格式

代码	值
CLA	80
INS	CA
P1	9F
P2	4F
Le	00

c) 如果命令的返回状态字不是“9000”，则读卡器产生“卡未被接受”的返回代码，并终止交易日志读取过程；

d) 读卡器验证日志格式（9F4F）是否存在。如果日志格式不存在，则读卡器产生“卡未被接受”的返回代码，并终止交易日志读取过程；

e) 读卡器验证日志格式是否包含卡需要显示的标签。如果日志格式不包含需要的标签，则读卡器产生“卡未被接受”的返回代码，并终止交易日志读取过程；

f) 读卡器发出“读取记录”指令去读取交易日志的下一个记录（短文件标识符 SFI 为“0B”的文件）。见表 C.9 用于获取日志条目的命令格式；

表C.9　用于获取日志条目的命令格式

代码	数值
CLA	00
INS	B2
P1	n（记录号）
P2	5C

Le	00

g) 如果卡返回的状态字节不是“9000”或“6A83”，则读卡器产生“卡未被接受”的返回代码，并终止交易日志读取过程；

h) 如果读卡器返回状态字节“6A83”，则读卡器已经将卡交易日志中所有有实际意义的记录读出；

i) 如果返回数据长度不是期望长度，则读卡器产生“卡未被接受”的返回代码，并终止交易日志读取过程；如果返回信息的长度为期望长度，则读卡器将响应报文复制到交易日志输出字符串中；

j) 读卡器继续读取下一日志条目，直到所有交易记录已被读出。

C.3.2.2 滚读显示交易日志

读卡器用“显示交易日志”过程来显示通过“读取交易日志”过程从卡中读到的交易日志。

显示交易日志处理有两个输入参数：

——表示交易日志中条目数的整数值 n；

——包含交易日志的二进制字节串。

交易日志的条目数由FCI中的标签所定义，表示交易日志的大小。相关定义见JR/T 0025.6—2018的B.1。

显示交易日志过程的唯一输出参数是返回代码。该返回代码的值为“成功”或“失败”。

读卡器进行以下动作，来执行交易日志显示过程：

a) 如果交易日志中的条目数为“0”，则读卡器提示持卡人目前没有交易日志信息，并停止显示交易日志过程；

b) 如果有交易日志信息，读卡器就会从每个交易日志条目中取得以下信息：

- 交易日期；
- 交易时间；
- 授权金额；
- 其他金额；
- 终端国家代码；
- 交易货币代码；
- 商户名称；
- 交易类型；
- 应用交易计数器（ATC）。

c) 如果密文信息数据的 b8 和 b7 位被设为‘00’，则读卡器拒绝针对本条记录的交易，且不显示其交易日志细节，读卡器继续处理下一条记录；

d) 读卡器宜构造包含以下数据元的显示字符串：

- 交易日期；
- 交易货币代码：在向持卡人显示之前，读卡器将交易货币代码的数字编码形式转换成字母编码格式（应符合 GB/T 12406 的规定）；
- 授权金额：包括小数。

显示字符串格式化为以下形式：日期——货币——金额。

之后读卡器处理下一条目。

C.3.3 圈存日志

C.3.3.1 读取圈存日志

读卡器逐条读取圈存日志过程在圈存日志查询时从卡片读取圈存日志。对于一次性读取全部圈存日志的功能是为发卡行进行圈存对帐提供参考，本部分不做具体规定。

表C.10列出了为实现读取圈存日志过程，终端应定义的标签。

表C.10　读取圈存日志的终端（定义）标签

标签	类型	描述
84	B	DF 名称
DF4F	B	圈存日志格式

读取圈存日志过程返回以下输出参数：

——表示圈存日志中条目数的整数值（n）；

——返回的代码；

——包含圈存日志条目的二进制字符串。

圈存日志组织为记录列表形式，其中第1个记录包含写进文件的最后一条记录。假定每条记录的长度为M，表C.11描述了圈存日志是如何组织的。

表C.11　圈存日志的组织形式

字节	圈存日志
0	圈存日志的最后一个条目
M	圈存日志的倒数第 2 个条目
2M	圈存日志的倒数第 3 个条目
…	…

本部分的表10和表11描述了圈存日志条目的格式。

读取圈存日志的过程如下：

a) 读卡器选取卡应用程序。如果卡应用程序的返回代码不是“成功”，则读卡器停止圈存日志的读取，并产生“卡未被接受”的返回代码，否则读卡器从 SELECT 命令中获取的 FCI 数据中获取圈存日志入口（DF4F），以判断卡片是否支持圈存日志，以及可能包含的最大记录数；

b) 读卡器发出 GET DATA 命令取得圈存日志格式（DF4F）。表 C.12 描述了可使用的命令；

表C.12　用于取得圈存日志格式的命令的格式

代码	值
CLA	80
INS	CA
P1	DF
P2	4F
Le	00

c) 如果命令的返回状态字不是“9000”，则读卡器产生“卡未被接受”的返回代码，并终止圈存日志读取过程；

d) 读卡器验证圈存日志格式（DF4F）是否存在以及其值的长度。如果圈存日志格式不存在或其值的长度为零，则表明卡片不记录表 11 中定义的数据元（即表 10 中序号 5 的数据长度为 0）；

e) 读卡器发出“读取记录”指令去读取圈存日志的下一个记录。表 C.13 定义了可用于获取日志条目的命令格式；

表C.13　用于获取日志条目的命令格式

代码	数值
CLA	00
INS	B2
P1	n（记录号）
P2	64
Le	00

f）　如果卡返回的状态字节不是“9000”或“6A83”，则读卡器产生“卡未被接受”的返回代码，并终止圈存日志读取过程；

g）　如果读卡器返回状态字节“6A83”，则读卡器已经将卡圈存日志中所有有实际意义的记录读出；

h）　如果返回数据长度不是期望长度，则读卡器产生“卡未被接受”的返回代码，并终止圈存日志读取过程；如果返回信息的长度为期望长度，则读卡器将响应报文复制到圈存日志输出字符串中；

i）　读卡器继续读取下一日志条目，直到所有交易记录已被读出。

C.3.3.2　滚读显示圈存日志

读卡器用“显示圈存日志”过程来显示通过“读取圈存日志”过程从卡中读到的圈存日志。

显示圈存日志处理有两个输入参数：

——表示圈存日志中条目数的整数值 n；

——包含圈存日志的二进制字节串。

显示圈存日志过程的唯一输出参数是返回代码。该返回代码的值为“成功”或“失败”。

读卡器进行以下动作，来执行圈存日志显示过程：

a）　如果圈存日志中的条目数为“0”，则读卡器提示持卡人目前没有圈存日志信息，并停止圈存日志显示过程；

b）　如果有圈存日志信息，读卡器应从每个圈存日志条目中，解析出表 10 和表 11 定义的信息；

c）　读卡器宜将表 10 和表 11 定义的信息格式化为当地通用语言或持卡人可识别的语言的字符串，并显示出来；

d）　读卡器处理下一条目。

附 录 D
（资料性附录）
电子现金简介

D.1 概述

D.1.1 市场背景

目前的银行卡交易基本采用联机授权方式。然而联机授权有时可能因为以下原因而无法实现：

——缺少联机环境（如自动售货机）；

——通信连接不可靠（如通信困难地区）；

——用于交易授权的费用不够经济（如对于小额支付）。

针对高风险持卡人市场用户群，电子现金（EC）可提供解决上述问题的方案和相关的应用规划。

D.1.2 电子现金介绍

本附录定义了电子现金解决方案，介绍成功实现电子现金方案的必要条件，并描述电子现金环境和传统借记/贷记环境之间的区别。

电子现金方案采用发卡行配置的可进行脱机交易授权的金融IC卡，确保对脱机风险的完全控制，防止从持卡人账户中透支余额。采用电子现金方案，银行可以：

——从当前账户中（借记或贷记账户）划出一部分金额；

——在支付卡内保存此额度信息；

——使卡可无借贷风险的脱机使用，直到划入的金额用完或再充值。

电子现金解决方案是基于完全兼容借记/贷记应用的支付产品组件，并具有标准借记/贷记应用的高级风险管理特性。

电子现金可为借记/贷记卡用于脱机交易提供一种新的技术解决方案，他的灵活性表明其具有更广泛的应用性，且可用于更多领域的应用。

D.1.3 电子现金为发卡行带来的利益

电子现金是一种强有力的解决方案，他可为发卡行带来以下显著利益：

——芯片提供的高级风险管理机制，允许发卡行在更多的细分市场发卡而不增加风险[5)]；

——电子现金方案的灵活性，帮助银行在基于芯片风险管理方面的投资多元化[6)]。

电子现金解决方案尤其适用于需要部分地进行脱机交易而不增加额外风险的借记/贷记卡。

电子现金也可作为一个独立的应用与借记/贷记应用共处一张卡上，此时电子现金应用可专门用于脱机状态下的小额支付。

D.2 商业契机

D.2.1 新的持卡人用户群

5) 这将帮助发卡行聚集更多的存款额，因为原本以现金进行的交易被以卡进行的交易所替代。

6) 这种情况下可以先发卡，之后再逐步实现发卡行系统功能，以获取从磁条向芯片技术迁移所带来的好处。

具有电子现金功能的金融IC卡可安全地向以下新市场发行：对银行业务较为陌生、未达到银行卡业务要求的用户群。所有这些都意味着一个潜在巨大的储蓄池，银行可用于再投资以获取利息收入。

欲拓展这些新市场的银行面临的问题是，坏债与欺诈风险更高。对于标准借记/贷记用户来说，这种风险通过所有交易联机授权来进行管理。然而这种花费是昂贵的（尤其对于大部分交易均为小额支付的场所来说），此外针对具有小额存款的用户，银行对账户的操作费用已超过了赚取的收入。针对这种问题，银行曾实施过各种应对措施，如专用卡、ATM卡、仅限直联交易的卡产品，但他们也同时限制了用户的使用。具有电子现金功能的金融IC卡可解决这些问题，因为他能让发卡行有效控制风险，且可将操作费用降至最低程度。

D.2.2 具有电子现金功能的金融IC卡的优点

具有电子现金功能的金融IC卡的优点及原因如下：

——低坏债风险：所有资金经过预先授权；

——低欺诈风险：金融 IC 卡非常安全，难以伪造且卡具有完善的脱机风险管理处理；

——低成本：通信成本、主机处理成本以及对账户的操作成本都减到最小。

在电子现金方案中，银行可通过向未达到银行卡业务要求的用户提供一个简单账户，来发展这部分用户群。该简单账户仍然支持POS终端的卡支付，客户不太可能取走所有存款，这样该账户相对来说能给发卡行带来更多的收益。

对于该持卡人群来说，使用具有电子现金功能的金融IC卡的另外一个关键优点是，由于他基于借记/贷记应用，可以自然升级至全借记或全贷记产品而无需再次发卡。

D.2.3 新的受理环境

由于具有电子现金功能的金融IC卡可以脱机授权，因此可通过在一些主要是脱机交易的场所（如自动售货机、加油站或停车位等）进行卡支付交易来增加授权金额，替代现金。

这将为卡支付产生一个新的、巨大的市场，尤其是和电子现金的小额支付特性相结合时（见D.2.4）。

这些新的可能的受理点包括现有的借记/贷记应用终端，这些终端可以受理标准的借记/贷记应用，加以改造后可受理电子现金交易。

D.2.4 小额支付

电子现金由于以下原因而显得非常经济：

——更小的欺诈和坏债可能性；

——更低的通信花费；

——网络不稳定时造成的影响更小；

——账户操作的成本更低；

——交易量增长而无需相应追加中央处理系统的投资，更加经济。

这种经济性意味着，可以用更低廉的成本处理卡支付，并且可以部分替代现金交易。这是一个非常重要的契机，因为目前基于现金支付的消费额仍远远超过基于卡支付的消费额。通过在更多领域实施卡片支付，可以降低消费流通领域的支付成本。

D.3 电子现金特性

D.3.1 实现特征

电子现金解决方案的典型实现特征包括：

——卡片保存余额（或预先授权额度），因此脱机交易不会导致透支风险；
——卡片具备增强的脱机风险管理功能，这一点通过将脱机风险限制在发卡行的定义范围内来实现；
——使卡片用于小额支付在经济性上更具吸引力。

D.3.2 电子现金余额

我们在讨论电子现金时使用“电子现金余额”这一术语，他表示使用该卡支付时，发卡行承诺给用户用于后续脱机支付的剩余额度。

根据持卡人的选择，可允许通过POS或ATM，或一些如电子现金余额读卡器之类的手持设备，将该余额读出并显示。读取电子现金余额的功能可在个人化时关闭。

D.3.3 发卡行主机端锁定的金额

为确保卡中用于将来脱机消费的金额不被持卡人挪作他用，当卡圈存的时候，电子现金方案需要进行某种形式的金额冻结。

该特性的细节实现完全取决于发卡行如何定位用户的需求，取决于每个主机系统的实现细节。为获得期望的结果，可能采用以下机制：

——从主账户余额中划出电子现金额度；
——将电子现金额度标识为与主账户关联的一个映射账户，将金额从当前账户移至映射账户；
——关于电子现金方案对发卡行主机系统影响的更多细节，在本部分中给出。

D.3.4 POS终端受理

由于具有电子现金功能的金融IC卡中的软件是借记/贷记应用兼容的，因此该卡可用于所有支持借记/贷记应用的芯片终端。

在通常的借记/贷记处理过程中，卡与终端均执行风险管理功能。只要符合条件就执行脱机交易，但出现以下任何一种情况时，需请求联机授权：

——授权金额超出终端最低限额；
——授权金额超出电子现金余额；
——终端对所有的交易处理都联机进行（即终端最低限额为“0”）；
——交易过程中产生错误，强制联机授权；
——尝试了芯片技术但工作不正常（“技术降级”）。

任何终端可以实现余额与交易日志显示功能，但对POS终端，这些功能不作强制要求。

D.3.5 圈存处理

卡的日常使用必将耗尽其中的电子现金余额，因此应对电子现金余额进行充值。增加电子现金余额的操作即称之为“圈存”操作。圈存交易包括以下两个操作：

——资金预先授权；
——卡片充值。

圈存操作一般在一些特定的终端上进行，该终端除要求与JR/T 0025—2018兼容外，应支持以下特性：

——能够与发卡行主机系统进行联机对话；
——支持相应的持卡人操作界面；
——通常在终端与发卡行主机间建立私有对话，以管理更新命令的发送与接收。

对于ATM或银行柜面的终端来说，只要加载合适的软件，便成为一个很好的圈存终端。

圈存操作如何进行取决于所选择的实现方式。持卡人可自己完成该过程，也可由发卡行进行自动圈存。要实现自动圈存，发卡行与持卡人之间需签订一份（同意自动圈存的）协议。在满足预定条件时，由发卡行划入额外金额，并对卡片的电子现金余额进行自动更新，而无需持卡人的介入。

电子现金金额转入的结果是，将金额转入由发卡行主机保存的“电子现金账户金额”（见本部分7.2）。

当对电子现金账户进行圈存后，发卡行应更新卡中相应的计数器以反映这种改变，从而增加卡电子现金余额。

D.3.6 磁条交易

电子现金是基于芯片的产品，最佳适用于金融IC卡终端较为普及的地区。在仅配备了支持磁条终端的地区，则使用卡片上的磁条进行交易，因为具有电子现金功能的金融IC卡是复合卡。

磁条交易不影响卡的电子现金余额。

D.3.7 清算

收单行以与对待标准借记/贷记交易相同的方式处理电子现金交易。已被脱机批准的交易需按常规方式提交清算。然而，由于是芯片产品，发卡行可能收到关于交易的一些额外信息，包括交易证书。

发卡行一般针对从账户余额中冻结的金额来处理清算记录。对于发卡行来说，清算是将联机余额与卡中脱机计数器进行再同步的一次机会。

D.3.8 交易货币

在电子现金交易中，授权金额是从卡中可供脱机消费余额中扣减的一个准确值，因此该值是否准确很重要。出于这个原因，如果卡要实现持卡人账户的“零透支”，具有电子现金功能的金融IC卡就不能支持货币转换功能，所有脱机交易应使用应用货币。

D.3.9 交易日志

具有电子现金功能的金融IC卡应用可将卡最近交易的信息，记录至交易日志中。相应的终端或手持读卡器可读出该日志，并显示或打印出记录，持卡人因此可从中了解其最近的交易历史。

D.3.10 电子现金的范围

电子现金方案最适合工作于封闭系统。发卡行需要与收单行就实现电子现金相关的一些特定功能，取得一致性协议，包括：

——余额显示；

——确保某些功能的完整性，如在非发卡行终端机的圈存功能。

具有电子现金功能的金融IC卡仍有可能超出该封闭系统使用，但这种情况下持卡人的体验可能不同于在封闭系统中使用。发卡行需要充分意识到这一点，并对其持卡人作相应的培训。