ICS 03.220.20；35.240.15
R 07

JT

中华人民共和国交通运输行业标准

JT/T XXXXX—XXXX

交通一卡通二维码支付技术规范

Technical specification for two-dimensional code payment of transport card

（征求意见稿）

（本稿完成日期：2017-10-10）

XXXX-XX-XX 发布　　XXXX-XX-XX 实施

中华人民共和国交通运输部　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交通运输部运输服务司提出。

本标准由交通运输信息通信及导航标准化技术委员会归口。

本标准起草单位：中国交通通信信息中心以及北京中交金卡科技有限公司，协作单位为北京中交信联认证有限公司、北京市政交通一卡通有限公司、福建交通一卡通公司、北京握奇数据系统有限公司、中国软件与技术服务股份有限公司、北京中电华大电子设计有限责任公司、北京中广瑞波科技股份有限公司、深圳市雄帝科技股份有限公司、无锡华捷电子信息技术有限公司、浙江蚂蚁小微金融服务集团股份有限公司。

本标准主要起草人：王一路、汪宏宇、李岚、王孝广、康雪、郎莹、李硕、惠思涌、沈伟彬、王晶、邢钊、罗贯伟、许高明、臧宏伟、崔文文、李晓波、沈凌楠。

交通一卡通二维码支付技术规范

1 范围

JT/T XXXX规定了交通一卡通二维码支付的应用场景、体系框架及流程、数据结构、信息接口、安全要求、终端要求、客户端软件要求以及检测项目。

本标准适用于交通运输行业二维码支付的相关系统、终端、手机客户端的设计与研发。

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，仅所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 18284-2000 快速响应矩阵码

GB/T 2312 信息交换用汉字编码字符集·基本集

GM/T 0003 SM2 椭圆曲线公钥密码算法

GM/T 0004 SM3 密码杂凑算法

JT/T 978.3-2015 城市公共交通 IC 卡技术规范 第 3 部分：读写终端

JT/T 978.4-2015 城市公共交通 IC 卡技术规范 第 4 部分：信息接口

JR/T 0025.7-2013 中国金融集成电路（IC）卡规范 第7部分：借记/贷记应用安全规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

二维码 two-dimensional code

用与二进制数据相对应的图形来表示数据信息的几何形体。

3.2

交通一卡通二维码支付体系 two-dimensional code payment system of transport card

交通一卡通发行二维码用于支付所涉及到的运营方、系统和受理终端等的统称。

3.3

发码平台 publishing two-dimensional code platform

支持生成交通一卡通互联互通二维码、认证用户身份、控制二维码生成与交易风险等功能，确保二维码及支付安全性的平台。

3.4

发卡机构 cardissuer

发行城市公共交通卡，并对清分结算的跨机构交易数据进行验证的机构。

3.5

收单机构 acquirer

布放交通一卡通二维码终端，为交通一卡通二维码提供扫码、资金结算服务，并对清分结算的跨机构交易数据进行收集、上传的机构。

3.6

受理终端 terminal

可识别和受理二维码的终端设备。

3.7

公钥 public key

非对称密钥对中公开的密钥。

3.8

私钥 private key

非对称密钥对中非公开的密钥。

4 缩略语

下列缩略语适用于本文件。

HTTPS：超文本安全传输协议（Hyper Text Transfer Protocol over Secure Socket Layer）；

QRCode：一种矩阵二维码符号（Quick Response Code）

SM2：国密算法2，即椭圆曲线公钥密码算法（PublicKey Cryptographic Algorithm SM2 Based on Elliptic Curves）；

SSL/TLS：安全套接层（SecureSocketsLayer）/传输层安全（TransportLayerSecurity）；

TLV：标签、长度和值（Tag Length Value）；

USB-HID：直接与人交互的设备（UniversalSerialBus-HumanInterfaceDevice）。

5 应用场景

交通一卡通二维码支付主要是应用于公共交通行业内公交、地铁等场景。采用被扫模式，即受理终端（以下简称：终端）扫码用户使用智能手机中安全客户端软件生成交通一卡通互联互通二维码。

6 支付体系架构及流程

6.1 体系架构

交通一卡通二维码支付体系架构中系统组成如下：

a) 证书管理中心的CA管理系统：负责为入网机构签发机构公钥证书，此证书用于二维码互联互通使用；

b) 支付账户系统：负责对二维码消费行为进行记录和管理；

c) 二维码发码管理系统：负责生成二维码数据并将二维码数据下发到手机客户端；

d) 发码平台的CA管理系统：负责为用户分配公私钥；

e） 风控系统：根据用户交易情况、信用等级等进行风险控制，负责二维码发码安全管理；
f） 支付结算系统：为发行的二维码消费记录进行支付、结算等资金操作；
g） 发卡机构的 CA 管理系统：负责与证书管理中心的 CA 管理系统进行对接，提交发卡机构公钥证书请求文件、接收证书管理中心下发的发卡机构公钥证书等；
h） 交易计费系统：负责采集受理终端上传的原始交易数据，匹配进出站交易并根据计费规则计算交易金额；
i） 终端管理系统：负责与证书管理中心的 CA 管理系统进行对接，接收证书管理中心下发的机构证书、将证书下发至所有终端、管理终端软件更新、远程监控终端等；
j） 手机客户端：负责展示二维码数据、为用户提供界面展示、用户消费记录查询、账户信息查询等。

交通一卡通二维码支付体系结构见图 1。

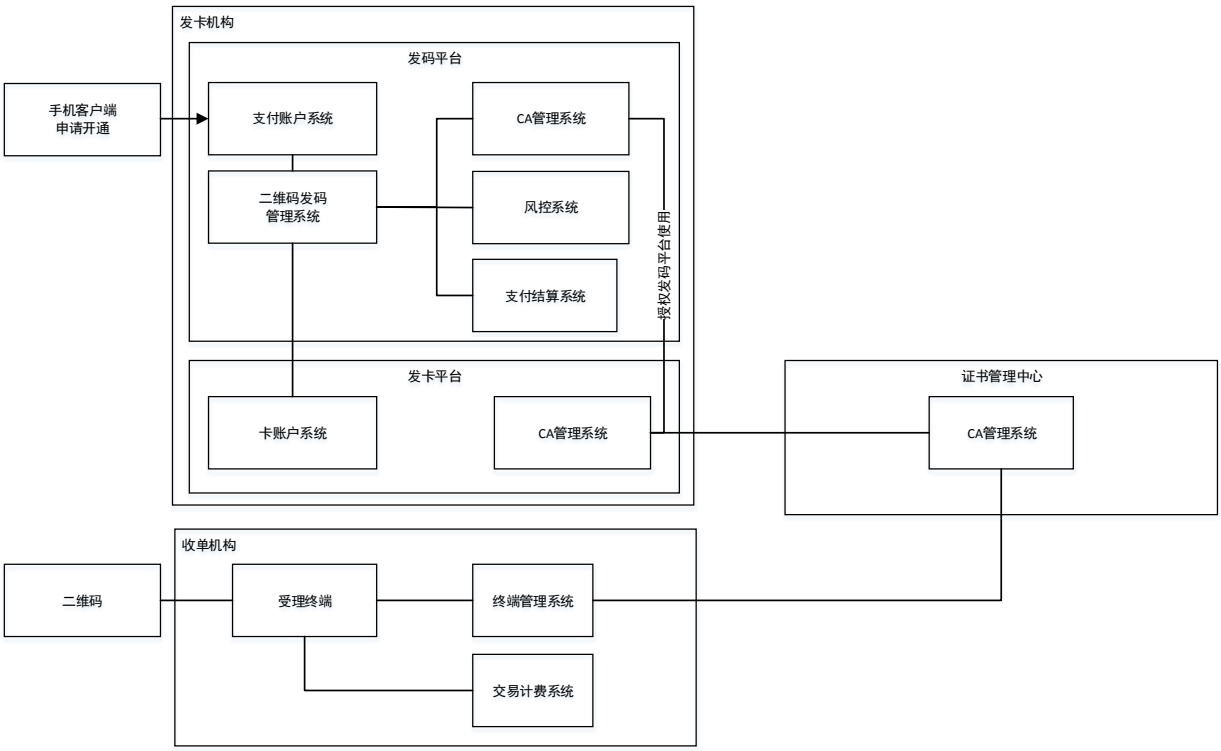


图1　交通一卡通二维码支付体系结构图

6.2　工作流程

交通一卡通二维码支付的工作流程如下：

a） 参与交通一卡通二维码支付的发卡机构 CA 管理系统应定时向证书管理中心的 CA 管理系统申请签发交通行业二维码支付互联互通的机构证书；
b） 证书管理中心的 CA 管理系统应将中心公钥证书下发至收单机构，收单机构负责将中心公钥证书下发至所有受理终端；
c） 二维码发码平台应评定账户的信用等级、风险等级等并综合各因素决定客户端可否生成二维码，还应根据用户账户信息、二维码有效期等因素生成二维码数据；

d) 用户持二维码进行扫码时，受理终端应验证二维码的真实性、有效性和完整性，成功识别二维码后进行记录，并将信息实时发送至系统后台；

e) 交易计费系统接收到终端上传的交易数据后，将进出站记录进行匹配，并计算交易金额，最终将统计好的异地交易数据上传至清分结算机构；

f) 清分结算机构的清分结算系统将跨区域交易数据转发至发卡机构，并对跨区域交易数据进行清分结算；

g) 发码平台根据发卡机构清分结算系统的用户消费情况进行记账，并完成支付结算；

h) 二维码数据上传过程中，系统间采用准实时交易传输且交易处理时间不超过 5 min。

交通一卡通二维码支付工作流程见图2。

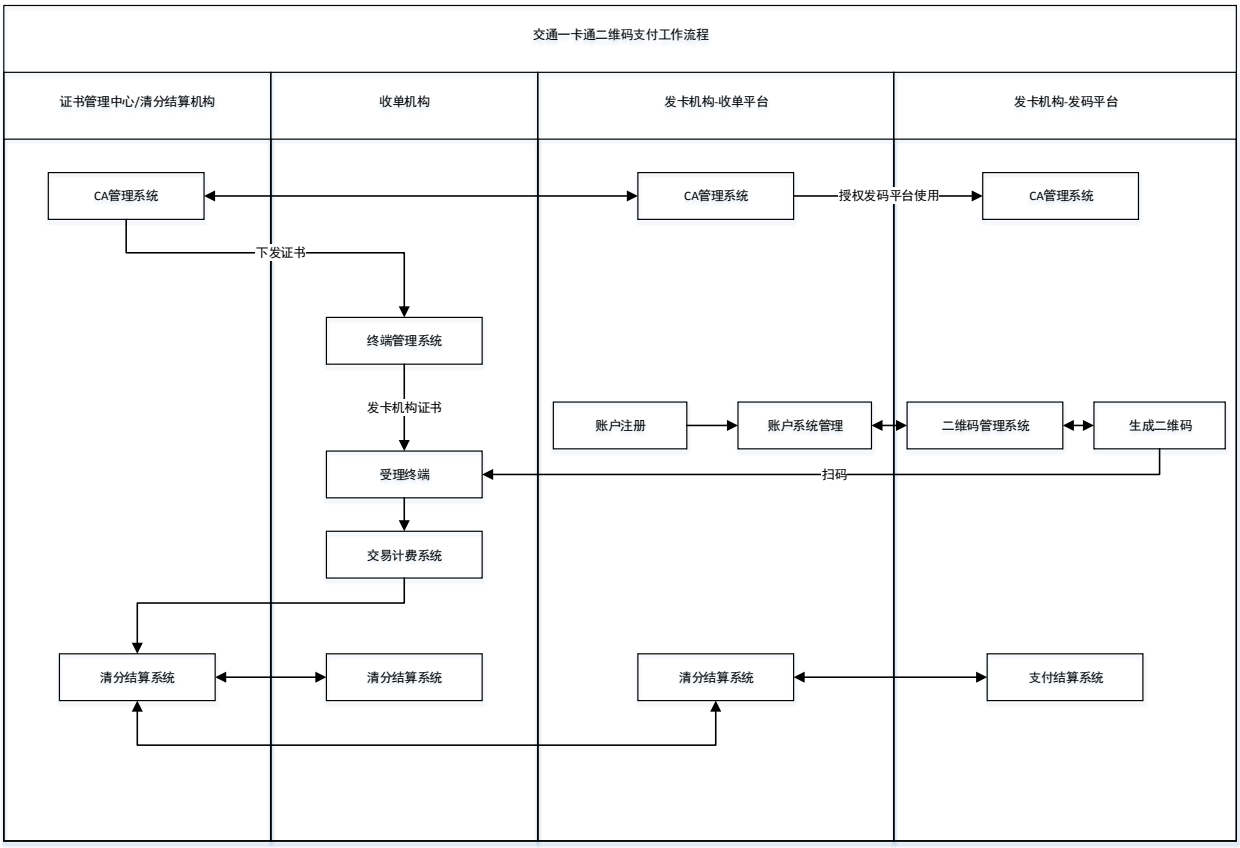


图2　交通一卡通二维码支付工作流程图

6.3　交易流程

交通一卡通二维码支付交易流程如下：

a) 客户端软件采集用户申请生成交通一卡通二维码的请求信息，包括用户账户信息等；

b) 客户端软件后台系统判断申请用户账户信息是否可以生成交通一卡通二维码；

c) 若后台系统判断允许用户生成交通一卡通二维码的，则后台系统生成交通一卡通二维码，并发送至客户端软件前端请求二维码展示；否则后台系统拒绝二维码生成请求，交易终止；

d) 客户端软件前端收到来自系统后台发送的二维码数据后，对二维码数据的完整性与有效性进行验证，若验证通过，则根据用户选择判断是否在客户端软件前端予以二维码展示，否则，则将生成的二维码存储在客户端软件的安全区域中。

注：交通一卡通二维码生成后，二维码的有效期根据用户展示时间而定，客户端软件应支持对二维码展示有效期的判断。

交通一卡通二维码支付交易流程见图3～5。

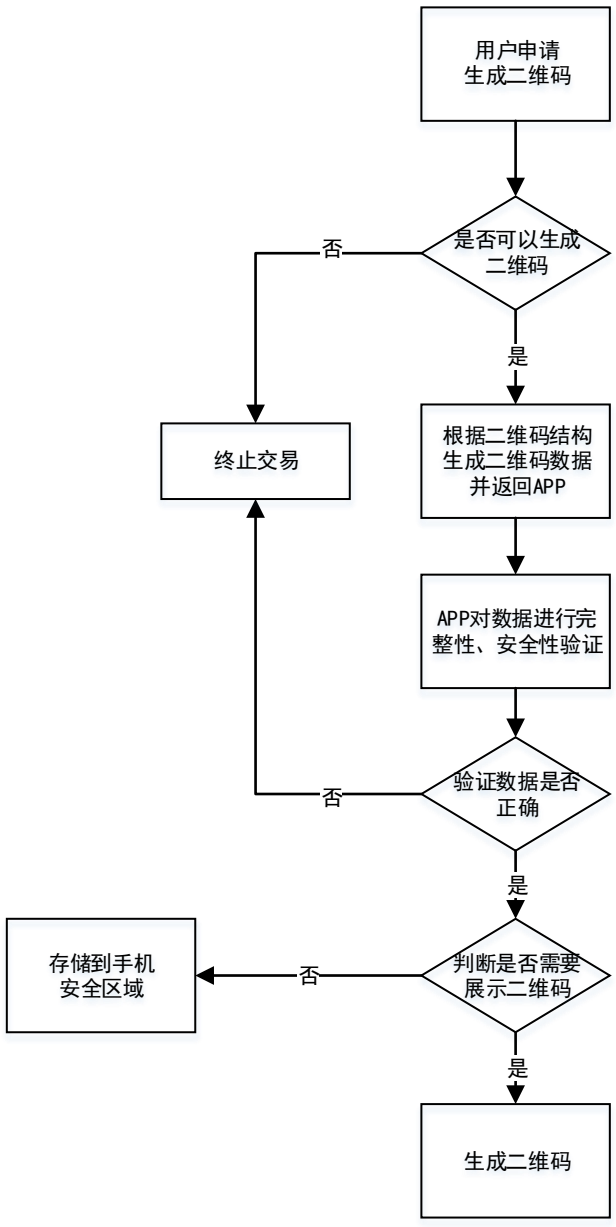


图3　申请交通一卡通二维码流程图

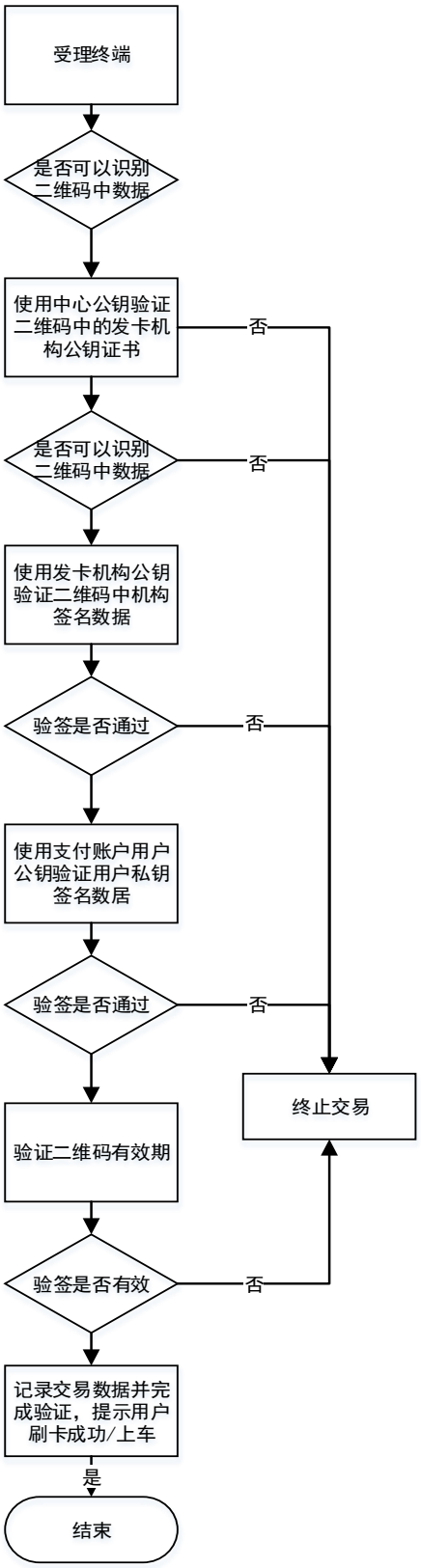
受理终端识别二维码验证流程如下：

a) 用户将生成交通一卡通二维码放置在受理终端二维码扫码处，受理终端读取二维码数据信息；

b) 受理终端调用存储在安全区域中的中心根公钥证书验证二维码数据中的发卡机构公钥证书，若能识别二维码数据，则使用识别到的二维码数据中的发卡机构公钥证书验证二维码数据中发卡机构私钥签名后的数据，否则，二维码验证交易终止；若发卡机构公钥证书验证二维码数据中发卡机构私钥签名的数据通过的，则获取到所有二维码数据信息，否则，二维码验证交易终止；

c) 在终端获取二维码数据后，验证二维码数据是否在使用有效期内，若在有效期内，受理终端记录二维码交易记录，并对交易成功或刷卡成功提示，否则二维码验证交易终止。

受理终端识别二维码验证流程见图 4。



注：验证二维码有效期包括发卡机构公钥证书有效期、支付账户系统授权过期时间、二维码有效期以及二维码生成时间。

图4　受理终端识别二维码验证流程图

跨区域交易清分结算流程说明如下：

a) 受理终端通过联网，将采集的二维码交易数据通过终端系统后台，上传至收单机构数据采集系统；
b) 收单机构数据采集系统根据二维码交易数据中的账户 ID、交易时间等数据信息进行匹配，并根据收单机构公共交通扣费，完成结算交易数据；
c) 收单机构清分结算系统对所有结算交易数据进行本地交易与异地交易判断，收单机构将跨区域异地交易数据上传至清分结算机构清分结算系统，交易数据上传数据格式要求见 8.7 的要求；
d) 清分结算机构清分结算系统将交易数据进行清分，并将相应的反馈文件下发至收单机构，将相应的结算文件下发至发卡机构；
e) 发卡机构根据收到的清分结算文件进行相应的结算处理。

跨区域交易清分结算流程见图 5。

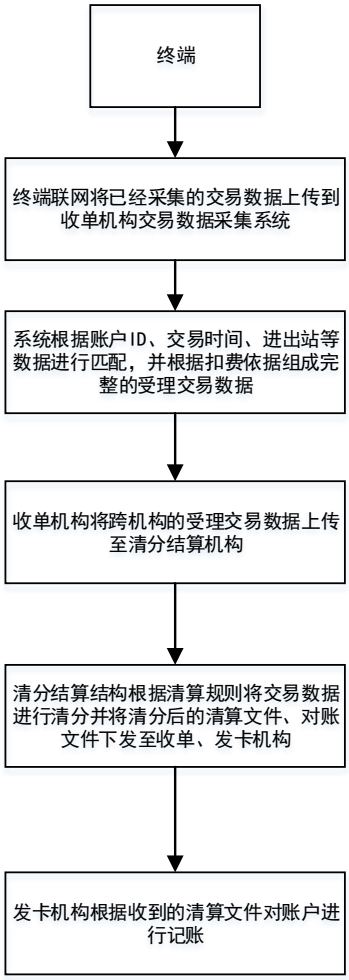
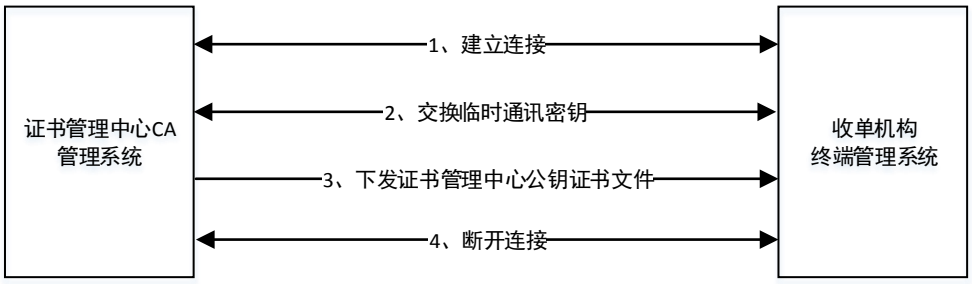


图5　跨区域交易清分结算流程图

6.4 证书管理中心根公钥证书下载流程

证书管理中心向收单机构下发根公钥证书流程见图6。

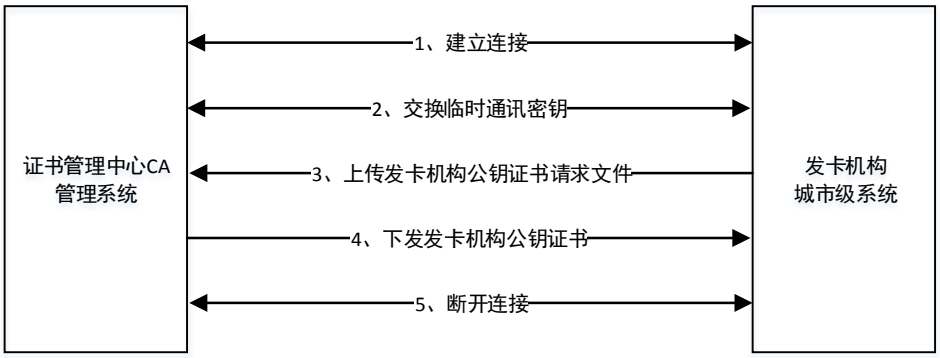


说明：证书管理中心与收单机构双方提前约定用于通讯保护的非对称密钥对，并交换公钥；

图6 证书管理中心公钥证书下载流程图

6.5 发卡机构申请机构公钥证书流程

发卡机构向证书管理中心请求发卡机构公钥证书流程见图 7。



说明：

a) 发卡机构根据 SM2 的要求生成用于二维码签名的公私钥对；

b) 证书管理中心与发卡机构双方提前约定用于通讯保护的非对称密钥对，并交换公钥。

图7 发卡机构申请机构公钥证书流程图

6.6 密钥工作流程

6.6.1 数据加密流程

交通一卡通二维码应使用发卡机构级密钥和发码平台用户级密钥对二维码数据进行加密，流程如下：

a) 支付账户系统为其用户分配的独立、不重复的一组或多组支付账户用户公/私钥对；

b) 用户密钥安全存储于手机客户端，并保证手机客户端和密钥存储的安全性；

c) 用户密钥存放于支付账户系统中，且以密文形式存储。

交通一卡通二维码数据加密流程见图 8。

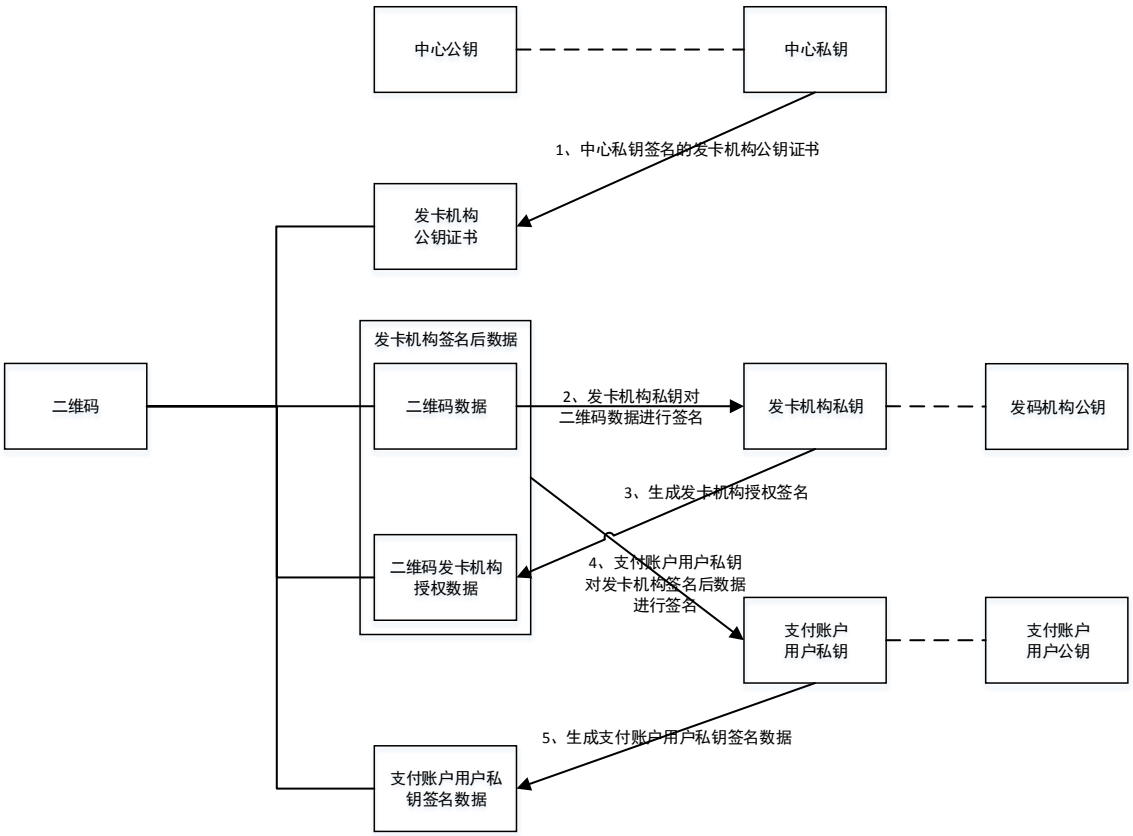


图8　交通一卡通二维码数据加密流程图

6.6.2　受理终端验签流程

受理终端验证交通一卡通二维码数据签名流程如下：

a)　受理终端使用证书管理中心的公钥验证发卡机构公钥证书的合法性和有效性；

b)　受理终端使用二维码中发卡机构公钥验证发卡机构授权签名数据的合法性和有效性；

c)　受理终端使用二维码中包含的支付账户用户公钥验证二维码中的支付账户用户私钥签名数据的合法性和有效性。

受理终端验证交通一卡通二维码数据签名流程见图 9。

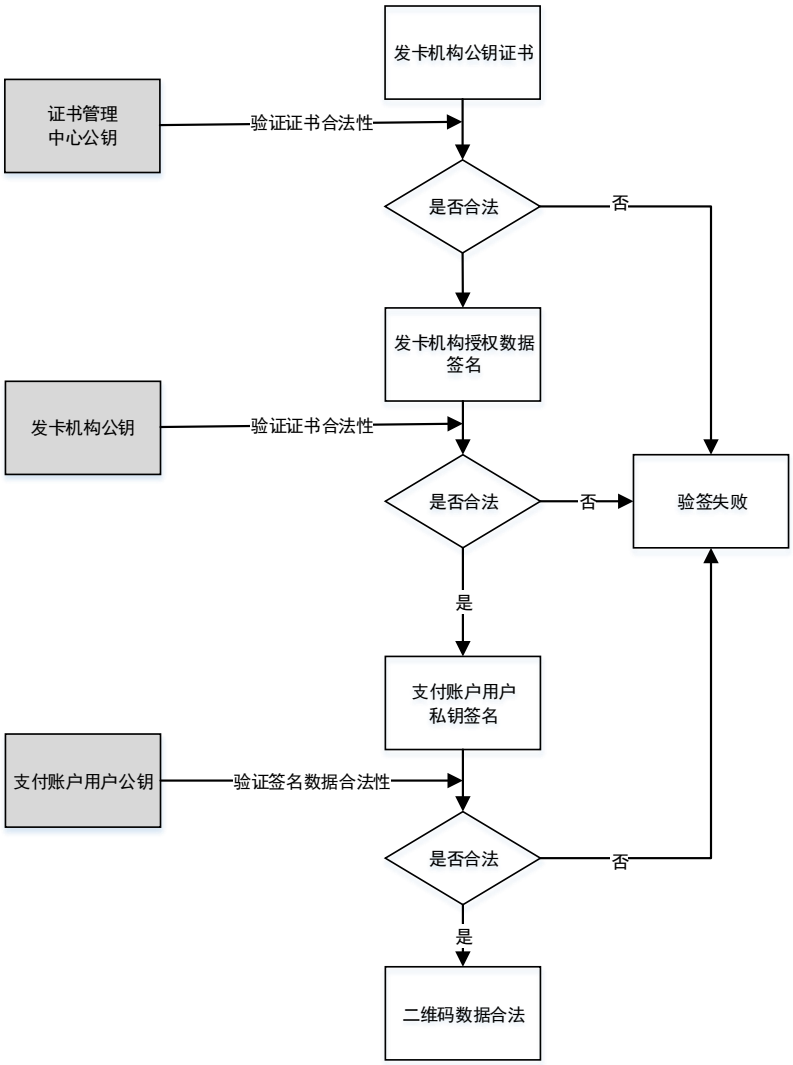


图9　受理终端验证交通一卡通二维码签名流程图

7　二维码数据结构

7.1　结构组成部分

交通一卡通二维码结构主要由二维码版本、二维码数据长度、发卡机构公钥证书、支付账户号、卡账户号、发卡机构号、发码平台编码、卡账户类型、单次消费金额上限、支付账户用户公钥、支付账户系统授权过期时间、二维码有效时间、发卡机构自定义域、发卡机构授权签名、二维码生成时间和支付账户用户私钥签名组成，交通一卡通二维码结构见图 10。

二维码结构															
二维码版本	二维码数据长度	发卡机构公钥证书	支付账户号	卡账户号	发卡机构号	发码平台编号	卡账户类型	单次消费金额上限	支付账户用户公钥	支付账户系统授权过期时间	二维码有效时间	发卡机构自定义域	发卡机构授权签名	二维码生成时间	支付账户用户私钥签名
1	2	117	16	10	4	4	1	3	33	4	2	32	65	4	65

图10　交通一卡通二维码结构图

交通一卡通二维码数据总长度为 332～364 字节。二维码数据结构组成部分见表 1。

表1　交通一卡通二维码数据结构组成部分

序号	字段名	长度	描述	格式	是否必填
1	二维码版本	1	二维码版本号。 0x80～0xFF 交通一卡通二维码标准版本，当前版本为0x81	B	M
2	二维码数据长度	2	第3～17字段的总长度。	B	M
3	发卡机构公钥证书	117	发卡机构公钥证书内容见表4。二维码版本为0x81时包含此字段。	B	MC
4	支付账户号	16	由支付账户系统自定义。	ans	M
5	卡账户号	10	由发卡机构账户管理平台定义。	B	M
6	发卡机构号	4	由清分结算机构统一分配。	B	M
7	发码平台编号	4	由清分结算机构统一分配。	B	M
8	卡账户类型	1	卡账户号的类型。见JT/T 978.2中表A.1中发卡机构特殊数据元第20字节卡种类型。	B	M
9	单次消费金额上限	3	二维码支付单次消费金额上限，由支付账户系统根据当前用户消费状态进行授权。此域在单次消费交易时可作为能否乘车的判断依据。	n	M
10	支付账户用户公钥	33	经过压缩的支付账户系统中用户公钥数据，压缩方法见GM/T 0003。	B	M
11	支付账户系统授权过期时间	4	支付账户系统授权过期时间，使用UTC（0时区）时间1970年1月1日00:00:00到现在的秒数。	B	M
12	二维码有效时间	2	二维码有效时间，与二维码生成时间一起控制二维码有效时间。以秒为单位，此域在填写时无需带单位。	B	M
13	发卡机构自定义域长度	1	发卡机构自定义域数据长度，最大32	B	C
14	发卡机构自定义域	N..32	发卡机构自定义，由发卡机构自定义域。	B	C
15	发卡机构授权签名	65	发卡机构私钥签名，签名数据包括：本表中3～14字段。	B	M
16	二维码生成时间	4	二维码生成的时间戳，使用UTC（0时区）时间1970年1月1日00:00:00到现在的秒数。	B	M
17	支付账户用户私钥签名	65	支付账户用户私钥签名数据，签名数据包括：本表中1～16字段。	B	M

7.2　数据签名

使用 SM2 算法的数据签名见表 2。

表2　数据签名

字段名	长度	描述	格式	是否必填
签名的数据格式	1	十六进制，值为‘15’	B	M
数字签名	64	二维码中数据计算的SM2签名r||s	B	M

7.3 符号要求

二维码组成中出现的符号要求见附录A。

7.4 编码格式

交通一卡通二维码数据采用二进制（8bit-byte）编码方式，符合GB/T 18284的要求。

8 信息接口

8.1 接口框架

清分结算机构与发卡机构、收单机构在信息交互过程中的信息接口，包括文件接口、文件存取方式、通信方式，其信息接口框架见图 11。

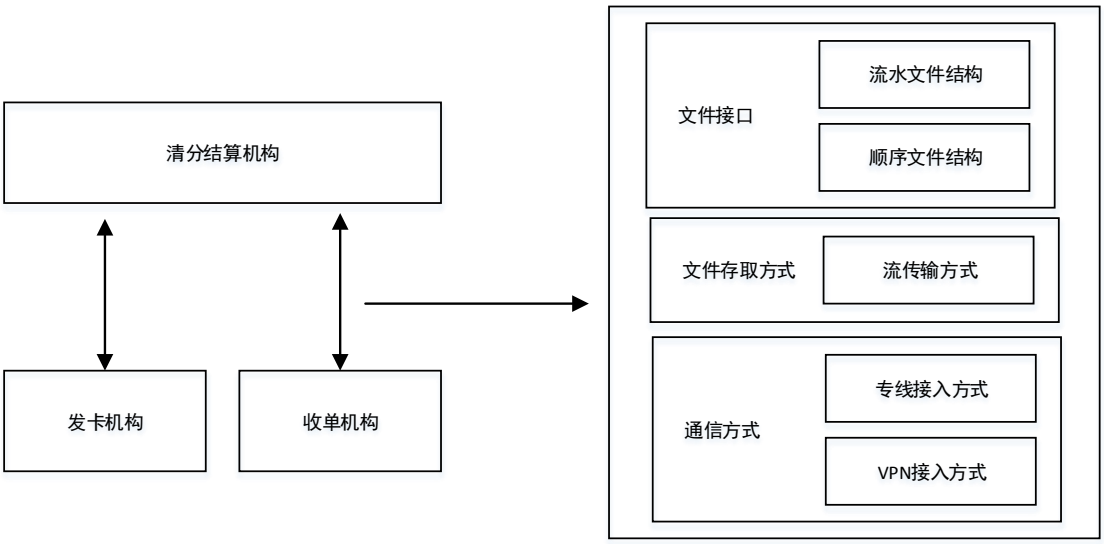


图11 信息接口框架组成

8.2 文件接口要求

8.2.1 文件结构

清分结算机构与发卡机构、收单机构间传输文件的文件存取方式包括流水文件结构和顺序文件结构。流水文件结构和顺序文件结构要求见JT/T 978.4-2015中的6.1。

8.2.2 文件类型

文件类型包括交易类和清算类，见表 3。

表3 文件类型

文件类型	文件名	文件标识	说明
交易类接口文件	二维码交易明细文件	BCPD/BCPR	收单机构上传的二维码消费明细文件。
清算类接口文件	二维码交易清算反馈文件	FB	消费清算反馈文件，反馈给收单机构。
	二维码交易清算明细文件	CL	下发给发卡机构的二维码消费清算明细文件。

8.2.3 接口报文交互流程

发卡机构、收单机构与清分结算机构间以流的方式进行文件传输，传输方式及报文要求见 JT/T 978.4-2015 中的 7.3。发卡机构、收单机构与清分结算系统间报文交换流程见图 12 和图 13。

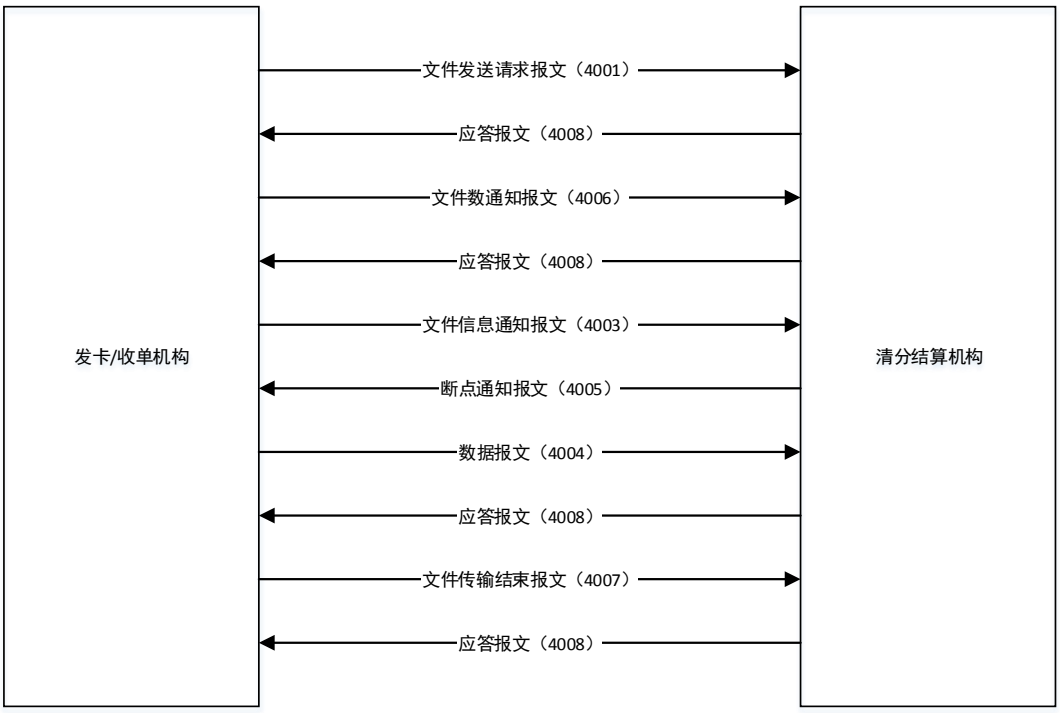


图12　上传文件交互流程图

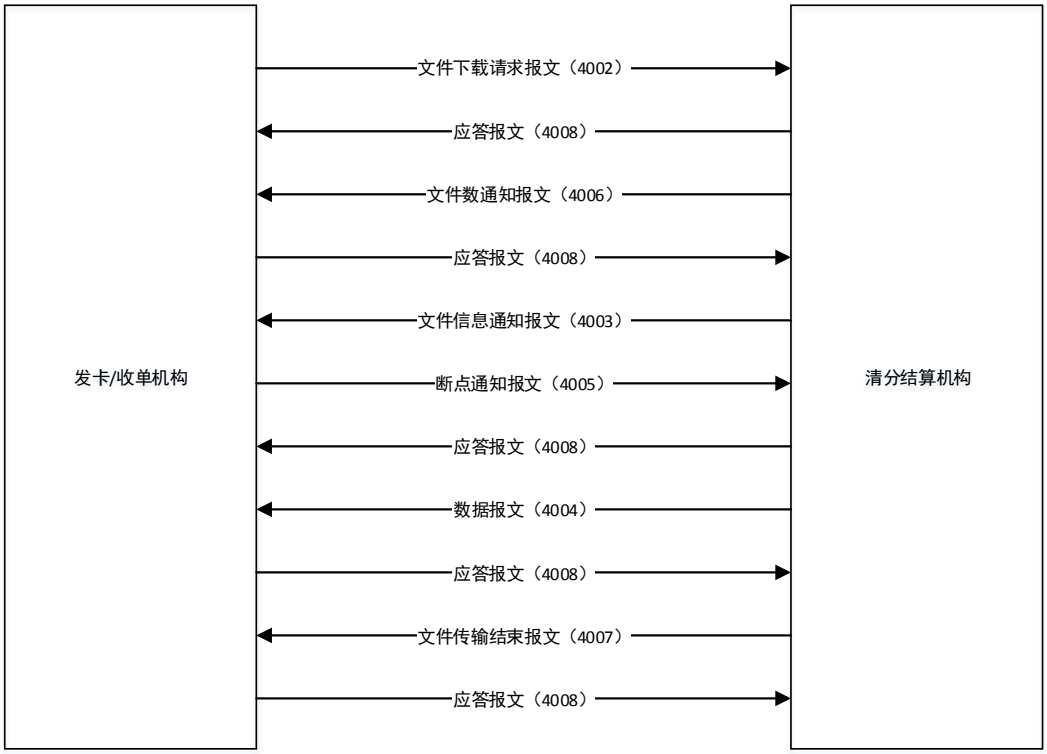


图13　下载文件交互流程图

8.2.4　交易记录文件命名规则

交易记录文件命名规则见表 4。

表4　交易记录文件命名规则

数据元说明	数据类型	长度（字节）	说明
文件标识	a	n	见表 5 中文件标志。
日期	n	12	年份用后两位，YYMMDDhhmmss
机构代码	n	8	清分结算机构分配
序列号	ans	10	机构自定义
文件标志	an	1	H：手工账；A：自动账

8.2.5　交易记录上传流程

交易记录应由收单机构交易计费系统根据受理终端上传的进出站记录整理，并计算出乘车的消费金额，然后将此记录上传至清分结算机构。

清分结算机构根据清算规则对交易记录进行清分结算，并将结果下发至相关机构。

发卡机构、收单机构与清分结算机构间系统对接时，应进行安全传输，并约定交易保护密钥及通讯保护密钥。

交易记录中出现的符号要求见附录 A。

8.2.6　交易记录结构

8.2.6.1　概述

交易记录是由交易记录头、交易记录体和交易记录尾组成。

8.2.6.2　交易记录头

交易记录头的内容见表 5。

表5　交易记录头

位置	长度	格式	内容（Outgoing）	内容（Incoming）	说明
0	3	n	交易代码	交易代码	常量：000
3	4	an	段位图	段位图	文件头记录只有一个段 0。
7	11	an	机构代码	机构代码	由发送方填写的机构代码，不足 11 位后补空格。
18	8	an	发送日期		格式为 YYYYMMDD
26	8	an	清算日期	清算日期	格式为 YYYYMMDD，机构上传时填写全 0，下发时清算中心填写
34	4	an	版本标记(TEST/PROD)	版本标记(TEST/PROD)	只允许填写 TEST 或 PROD 测试版本：TEST 生产版本：PROD
38	8	an	版本号	版本号	填写：00000001

8.2.6.3　交易记录尾

国际密钥体系交易记录尾内容见表 6。

表6　交易记录尾

字段名	长度	描述	格式	是否必填	说明
交易代码	3	标志记录尾的开始	n	M	由发送方填写，内容为001
段位图	4	段位图	an	M	标示段0是否存在

表 6（续）

字段名	长度	描述	格式	是否必填	说明
交易代码	3	标志记录尾的开始	n	M	由发送方填写，内容为001
段位图	4	段位图	an	M	标示段0是否存在
交易记录数	10	交易记录数	n	M	包括交易代码000、001在内的总记录数
MAK	16	交易激活密钥	an	M	MAC 密钥为 16 个 0～F 之间的 16 进制字符，A～F 应为大写。经过成员主密钥（MMK）加密保护。 按照MAC算法按JR/T 0025.7—2013，初始因子为：0000000000000000。
MAC	16	交易数据校验码	an	M	MAC为16个0~F之间的16进制字符，A~F应为大写。 按照MAC算法按JR/T 0025.7—2013，初始因子为0000000000000000。

国密密钥体系交易记录尾内容见表 7。

表7　交易记录尾

字段名	长度	描述	格式	是否必填	说明
交易代码	3	标志记录尾的开始	n	M	由发送方填写，内容为010
段位图	4	段位图	an	M	
交易记录数	10	交易记录数	n	M	包括交易代码000、010在内的总记录数
MAK	32	交易激活密钥	an	M	MAC 密钥为 32 个 0～F 之间的 16 进制字符，A～F 应为大写。经过成员主密钥（MMK）国密算法加密保护。
MAC	16	交易数据校验码	an	M	

8.2.6.4　交易记录体

交易记录体数据格式见表 8。

表8　交易记录体数据格式

字段名	长度	内容	格式	是否必填	说明
交易代码	3	标志记录体的开始。	n	M	386-二维码支付消费
段位图	4	段位图	an	M	标记记录体包含的段，段0必须包含，目前只有段0，值为8000。
消费类型	2	消费类型	n	M	消费类型： 00-单次消费； 01-复合消费。 02-系统补扣 （收单系统认定的追逃票交易）

表 8（续）

字段名	长度	内容	格式	是否必填	说明
扫码类型	2	扫码类型	n	M	扫码类型： 00-主动扫码，即用户使用手机扫描二维码； 01-被动扫码，即受理终端扫描用户生成的二维码。
系统跟踪号	6	受理机构向交易清分结算机构发送的每一笔交易，必须赋予一个交易流水号。	n	M	6 位定长数字字符
支付账户号	20	主账号	ans	M	不足右补空格
卡账户号	20	由发卡机构账户管理平台定义。	ans	M	
收单机构号	11	收单机构标志码。	ans	M	代码左对齐，不足 11 位右补空格
发卡机构号	11	发卡机构标志码。	ans	M	代码左对齐，不足 11 位右补空格
发码平台编号	11	发码平台标志码。	ans	M	代码左对齐，不足 11 位右补空格
商户类型	4	收单机构商户类型[表示商户分类编码（MCC）]	n	M	MCC 码
渠道类型	2	交易渠道类型	an	M	03-车载 POS 机
受卡方标识码	15	受卡方标识码	an	M	由 POS 终端管理机构分配的受卡方机构标识代码（商户代码，运营单位代码），右补空格。
受卡方名称地址	40	受卡方名称地址	an	M	受卡机构的名称和所在地（商户，运营单位的所在地），右补空格。
原始交易信息	23	原始交易信息，由清算机构填写	an	M	见表 9
清分结算机构流水号	12	由清分结算机构填写，入网机构填写 000000000000	n	M	由清分结算机构填写，入网机构填写 000000000000
交易金额	12	本域中不带小数点。交易金额为人民币的时候，本域的最后两位应包含人民币的角和分。	n	M	以分为单位
检索参考号	12		n	M	取值范围 000000000001～999999999999
收单机构流水号	12	收单机构流水号	n	M	由收单机构填写。
收单机构日期	8	收单机构上传交易日期	n	M	由收单机构填写。
货币代码	3	交易币种	an	M	人民币 156
优惠类型	4	优惠类型	an	M	默认 0000。
应收金额	8	应收金额	ans	M	用 8 个可见的 16 进制字符(0～9,A～F）表示。
算法标识	2			M	暂填写 00
保留域	32	保留使用	ans	M	全 F 填充

表 8（续）

字段名	长度	内容	格式	是否必填	说明
进站受卡机终端标识码	15	受卡机终端标识码	ans	M	受卡机具的终端标识
进站终端易序号	8	终端交易序号	an	M	用 8 个可见的 16 进制字符(0～9,A～F）表示。
交易摘要	128	交易的基本信息	ans	M	长度不超过 128 字节，如消费类型为 00 的交易：2017-12-31 19：00：00 运通 901 路，车号 3421，王府井 ； 消费类型为 01 的交易：2017-12-31 19：00：00 运通 901 路，车号 3421，王府井上车，2017-12-31 19：30：00 东单下车；消费类型为 02 的交易：2017-12-25 19：00：00 运通 901 路，车号 3421，王府井上车，2017-12-31 23：00：00 补扣。 不足右补空格。
进站时间	14	用户进站扫码时间。格式为 YYYYMMDDhhmmss	n	M	
出站受卡机终端标识码	15	受卡机终端标识码	ans	C	若无填写全 F，消费类型 01 必须填写正确的值
出站终端交易序号	8	终端交易序号	an	C	若无填写全 F，消费类型 01 必须填写正确的值
出站时间	14	用户出站扫码时间。格式为 YYYYMMDDhhmmss	n	C	若无填写全 F，消费类型 01 必须填写正确的值。 补扣交易填写系统补扣的时间，必须填写。
出站保留域	32	保留使用	ans	M	填写全 F
标签数据	VAR	可扩展标签数据	TLV	M	用于上送行业信息数据，此内容见 8.7.4。

表9　原始交易信息

长度	格式	内容
3	n	原始交易代码
10	n	原始交易的日期及时间（MMDDhhmmss）
6	n	原始交易的系统跟踪号
4	n	原始交易清算日期
结算交易时本字段以全零填充。		

8.2.6.5　TLV 规则

TLV 的第一个 T 的固定标签为 1000，用于指示标签信息。1000 后的 4 个字节代表后续数据的长度，可以为 0。不为 0 时 TLV 才会出现，标签示例参见附录 B。TLV 总长度不超过 4000（包括 TL）。

TLV 格式规则见表 10。

表10　TLV 格式规则

域号	长度	域名称	域类型	域取值	说明
1	4	T	ans	固定值 1000	
2	4	L	n	≥0	
3	VAR	V	an		由若干个标签代码连续组成根据业务需要定义，应和域 2 匹配

行业数据扫码信息标签代码见表 11。

表11　扫码信息标签代码

序号	标签代码	标签名称	格式	说明	是否必填
1	2001	上车扫码信息	HEX	上车二维码、终端及线路信息。	M
2	2002	下车扫码信息	HEX	下车二维码、终端及线路信息。单次消费交易、补扣交易此标签可为空。	M
3	2003	进站/上车时间	n	YYYMMDDHH24MISS	M
4	2004	出站/上车时间	n	YYYMMDDHH24MISS	M
5	2005	上车/进站线路/进口线路	ans		M
6	2006	下车/出站线路/出口线路	ans		M
7	2007	进站站点	ans		M
8	2008	出站站点	ans		M
9	2009	上车/进站终端号（闸机编号）	ans		M
10	2010	下车/出站终端号（闸机编号）	ans		M
11	2011	出发/上车城市号	ans		M
12	2012	到达/下车城市号/交易城市号	ans		M
13	2013	入口班次	ans		C
14	2014	出口班次	ans		C
15	2015	入口工号	ans		C
16	2016	出口工号	ans		C
17	2017	景区/点编码	ans		C
18	2018	司机号	ans		C
19	2019	检票员号/操作员号	ans		C
20	2020	从业资格证号	ans		C
21	2021	从业人员证件类型	ans		C
22	2022	从业人员证件号	ans		C
23	2023	交易门店号/网点号	ans		C
24	2024	采集点编号	ans		C
25	2025	等候时间	n	分钟	C
26	2026	行驶里程	n	单位：0.1 公里	C
27	2027	空驶里程	n	单位：0.1 公里	C
28	2028	空驶时间	n		C
29	2029	起步价	n	分	C

表 11（续）

序号	标签代码	标签名称	格式	说明	是否必填
30	2030	单价	n	元/公里	C
31	2031	出口号	n		C
32	2032	入口号	n		C
33	2033	联乘线路	ans		M
34	2034	换乘线路	ans		M
35	2035	联乘金额	n		C
36	2036	起步里程	n		C
37	2037	线路名称	ans	中文	M
38	2038	城市名称	ans	中文	M
39	2039	交通工具编号（车号）	ans		C
40	2040	交通公交类型	ans	枚举常量：BUS,BRT,LRT,METRO,FERRY	M
41	2041	车牌号	ans		C

8.2.6.6 扫码信息

终端扫描二维码成功后，应自动生成此扫码信息，并将扫码信息上传至系统后台。

扫码信息 TLV 规则见表 12，扫码信息标签定义见表 13。

表12 扫码信息 TLV 规则

域号	域名	格式	长度	说明
1	T	HEX	4	
2	L	HEX	4	
3	V		不定长	

表13 扫码信息标签定义

序号	标签代码	标签名称	格式	说明	是否必填	备注
1	0000	记录版本	HEX	脱机记录的版本	M	当前 0
2	0001	二维码	HEX	原始二维码信息	M	刷码识别的原始二维码信息
3	0002	终端厂商编号	HEX	终端厂商编号	M	终端入网检测时由检测机构分配
4	0003	终端编号	HEX	终端厂商下唯一编号	M	
5	0004	终端软件版本	HEX	终端软件版本号	M	终端生产的软件版本
6	0005	终端流水号	HEX	终端刷码流水号	M	
7	0006	商户类型	HEX	收单机构商户类型码	M	
8	0007	消费类型	HEX	00 单次消费 01 复合消费 02-系统补扣	M	系统补扣时，通常只有上车信息，在上车的标签中填写 02。
9	0008	币种	HEX	终端消费币种，消费类型为 00 时必传	C	156

表 13（续）

序号	标签代码	标签名称	格式	说明	是否必填	备注
10	0009	消费金额	HEX	终端交易金额，消费类型为 00 时必传	C	精度分
11	000A	车辆编号	HEX	当前终端对应的车辆号	C	
12	000B	车牌号	HEX	车牌号	C	
13	000C	司机编号	HEX	司机编号	C	
14	000D	线路信息	HEX	线路编号	M	
15	000E	站点编号	HEX	站点编号	C	
16	000F	经纬度	HEX	经纬度信息	C	
17	0010	终端时间	HEX	受理时间，1970-01-01 00:00:00 开始的秒数	M	
18	0011	完整性签名	HEX	2001/2002 标签的完整性签名	M	使用 GM/T 0004SM3 杂凑算法对除本标签外的其他标签计算摘要

8.2.7 交易清算反馈文件

8.2.7.1 概述

向收单机构下发当日清分结算机构对二维码交易的清算处理结果，供收单机构进行明细匹配。

8.2.7.2 文件格式

二维码交易清算反馈文件格式见表 14。

表14 二维码交易清算反馈文件格式

数据元说明	数据类型	长度	说明
文件说明区			
版本号	n	2	02
回车符	s	2	0x0D和0x0A
交易头			
记录总数	n	6	取值范围000001～999999
清分结算机构清算日期	n	8	YYYYMMDD
收单机构代码	n	11	右补空格
单笔交易长度	n	4	包含回车换行：取值范围0001～9999
保留域	ans	20	全F
回车符	s	2	0x0D和0x0A
交易数据体			
清分结算机构流水号	n	12	取值范围000000000001～999999999999
收单机构流水号	n	12	取值范围000000000001～999999999999
收单机构受理日期	n	8	YYYYMMDD
检索参考号	n	12	取值范围000000000001～999999999999
交易类型	an	4	
发卡机构清算机构标识	n	11	右补空格，发卡机构的清结算上级单位
发卡机构代码	n	11	右补空格，
收单机构清算机构标识	n	11	右补空格，收单机构的清结算上级单位
收单机构代码	n	11	右补空格，交易发生地机构代码
MCC	an	4	参考MCC文档

表 14（续）

数据元说明	数据类型	长度	说明
渠道类型	an	2	
卡账户号	n	20	不足右补空格
卡消费计数器	n	6	填充000000
保留金额	n	12	取值范围000000000000～999999999999
清算金额	n	12	取值范围000000000000～999999999999
交易日期	n	8	YYYYMMDD
交易时间	n	6	HHMMSS
错误代码	n	6	清分结算机构定义，取值范围000000～999999。
错误描述	ans	40	错误描述
测试标志	n	1	0为正式数据；1为测试数据。
手续费	ans	28	字段格式为小数，以分为单位，保留到小数点后7位，右补空格 例如：手续费为1.3333••••••元，字段应填写为： 133.3333333右补空格17位 手续费为0.123元，字段应填写为：12.3000000右补空格18位
发卡分润	ans	28	字段格式为小数，以分为单位，保留到小数点后7位，右补空格 例如：手续费为1.3333••••••元，字段应填写为： 133.3333333右补空格17位 手续费为0.123元，字段应填写为：12.3000000右补空格18位
收单分润	ans	28	字段格式为小数，以分为单位，保留到小数点后7位，右补空格 例如：手续费为1.3333……元，字段应填写为： 133.3333333右补空格17位 手续费为0.123元，字段应填写为：12.3000000右补空格18位
保留	ans	28	全0
保留域	ans	40	全F
回车符	s	2	0x0D和0x0A

8.2.8 二维码交易清算明细文件

8.2.8.1 概述

清分结算机构向发卡机构下发当日清分结算机构的清算结果，供发卡机构进行处理。

8.2.8.2 文件格式

二维码交易清算明细文件格式见表 15。

表15　CL 二维码交易清算明细文件格式

数据元说明	数据类型	长度	说明
文件说明区			
版本号	n	2	02
回车符	s	2	0x0D和0x0A
交易头			
记录总数	n	6	取值范围000001～999999
清分结算机构清算日期	n	8	YYYYMMDD
接收机构代码	n	11	右补空格
单笔交易长度	n	4	包含回车换行：取值范围0001～9999。
保留域	ans	20	全F
回车符	s	2	0x0D和0x0A
交易数据体			
清分结算机构流水号	n	12	取值范围000000000001～999999999999
收单机构流水号	n	12	取值范围000000000001～999999999999
收单机构受理日期	n	8	YYYYMMDD
检索参考号	n	12	取值范围000000000001～999999999999
交易类型	an	4	
收单机构清结算机构代码	n	11	右补空格，交易发生地单位
收单机构代码	n	11	右补空格，交易发生地单位
发卡地通卡公司代码	n	11	右补空格，发卡地
接收机构代码	n	11	右补空格，发卡地的顶级单位
发送机构标识码	n	11	右补空格，交易发生地的顶级单位
MCC	an	4	参考MCC文档
渠道类型	an	2	
卡账户号	n	20	不足右补空格
卡消费计数器	n	6	填充全0
交易金额	n	12	取值范围000000000000～999999999999
清算金额	n	12	取值范围000000000000～999999999999
交易日期	n	8	YYYYMMDD
交易时间	n	6	hhmmss
余额类型	an	1	0
算法标识	an	2	a)　01：3des b)　02：SM2 c)　04：SM4
错误代码	n	6	清分结算机构定义，取值范围000000～999999
错误描述	ans	40	错误描述
测试标志	an	1	a)　0：正式数据 b)　1：测试数据
手续费	ans	28	字段格式为小数，以分为单位，保留到小数点后7位，右补空格 例如：手续费为1.3333……元，字段应填写为：133.3333333右补空格17位 手续费为0.123元，字段应填写为：12.3000000右补空格18位

表 15（续）

数据元说明	数据类型	长度	说明
发卡分润	ans	28	字段格式为小数，以分为单位，保留到小数点后7位，右补空格 例如：手续费为1.3333……元，字段应填写为：133.3333333右补空格17位 手续费为0.123元，字段应填写为：12.3000000右补空格18位
收单分润	ans	28	字段格式为小数，以分为单位，保留到小数点后7位，右补空格 例如：手续费为1.3333……元，字段应填写为：133.3333333右补空格17位 手续费为0.123元，字段应填写为：12.3000000右补空格18位
发码方代码	ans	8	
保留	ans	20	
个性化数据，二维码扫码信息	ans		TLV格式，必选.首标签为1000标签。
回车符	s	2	0x0D和0x0A

8.3 文件存取方式

清分结算机构提供给发卡机构和收单机构的文件存取方式为流传输方式。流传输方式要求见JT/T 978.4-2015中7.3。

8.4 通信方式

清分结算机构与发卡机构、收单机构通信采用专线方式或VPN方式。

9 安全要求

9.1 密钥与算法

证书管理中心私钥对发卡机构公钥数据进行签名、发卡机构使用机构私钥对二维码数据进行签名以及支付账户系统用户私钥对二维码数据进行签名时使用的密码算法应符合 GM/T 0003 的规定。
受理终端验证证书、签名数据的合法性以及受理终端根据点压缩算法还原公钥数据时使用的算法应符合 GM/T 0003 的规定。

9.2 证书要求

9.2.1 发卡机构公钥证书请求文件

发卡机构向证书管理中心发送的公钥证书请求文件内容见表 16。

表16　发卡机构公钥证书请求文件

序号	字段名	长度	描述	格式	是否必填
1	记录头	1	十六进制‘23’	b	M
2	服务标识	4	标识一个交通服务，将相应应用的私有应用标识扩展(PIX)，右补十六进制‘0’构成 ‘01010000’ = 交通电子现金应用	b	M
3	证书格式	1	十六进制‘02’	b	M
4	证书失效日期	2	月和年(MMYY)，在该月最后一天之后证书失效	n4	M
5	记录号	3	发卡机构公钥证书申请记录号	n6	M
6	发卡机构公钥签名算法标识	1	标识发卡机构公钥签名算法。 ‘04’:SM2（16进制）	b	M
7	发卡机构公钥加密算法标识	1	标识发卡机构公钥加密算法，保留项 ‘04’:SM2（16进制）	b	M
8	公钥参数标识	1	用于标识椭圆曲线参数。默认为16进制‘00’	b	M
9	发卡机构公钥模长	1	33byte，采用SM2中点压缩方式进行计算。	b	M
10	发卡机构公钥	64	SM2 算法表示椭圆曲线上的一个点	b	M
11	数字签名	64	发卡机构使用其私钥对本表从1到10数据计算的 SM2 签名 r||s	b	M

9.2.2　发卡机构公钥证书

使用SM2算法,证书管理中心私钥对表3数据进行签名的证书数据格式,本部分总长度为117字节,见表17。

表17　发卡机构公钥证书

序号	字段名	长度	描述	格式	是否必填
1	记录头	1	十六进制值‘24’	b	M
2	服务标识	4	标识一个交通服务，将相应应用的私有应用标识扩展(PIX)，右补十六进制‘0’构成 ‘01010000’ = 交通电子现金应用	b	M
3	根 CA 公钥索引	1	根 CA 系统用来签发发卡机构公钥证书的公钥索引	b	M
4	证书格式	1	十六进制，值为‘12’	b	M
5	发卡机构标识	4	由证书管理中心统一制定并下发	cn 8	M
6	证书失效日期	2	MMYY，在此日期后，这张证书无效	n4	M
7	证书序列号	3	由根 CA 分配给这张证书的，唯一的二进制数	b	M
8	发卡机构公钥签名算法标识	1	标识发卡机构公钥签名算法 ‘04’：SM2（16进制）	b	M
9	发卡机构公钥加密算法标识	1	标识发卡机构公钥加密算法，保留项 ‘04’：SM2（16进制）	b	M
10	发卡机构公钥参数标识	1	用于标识椭圆曲线参数。默认为16进制‘00’	b	M
11	发卡机构公钥长度	1	标识发卡机构公钥的字节长度	b	M
12	发卡机构公钥	33	该字段是椭圆曲线上的一个点	b	M
13	数字签名	64	根 CA 对本表4至12项数据计算的 SM2 签名 r||s	b	M

9.3　存储安全

二维码支付交易中涉及关键、敏感数据需要进行安全保护，防止信息泄露和篡改。

9.4 通信安全

9.4.1 传输安全

二维码支付交易涉及各系统之间进行信息传输，各系统之间应建立安全通信信道，应对交易数据采用数字签名和加密等安全方式进行传输，确保数据不被监听和篡改，例如：基于 SSL/TLS 的 HTTPS 进行传输等。

公网环境下，二维码信息不应以明文形式传输。

9.4.2 传输数据的完整性

应具备对传输数据的鉴别机制，确保发出数据的完整性和接收数据具有完整性的校验。

9.4.3 传输数据的保密性

应对传输的数据进行保密性保护，不应引起信息泄露。

9.5 信息安全

二维码支付过程中涉及的信息安全应符合如下要求：

——二维码支付业务开通过程中账户及个人信息不被泄露；

——二维码数据防止重放；

——在使用过程中验证二维码的完整性、真实性、时效性，未通过验证的二维码数据不应予以使用。

9.6 支付安全

用户支付过程中涉及的安全要求如下：

a) 二维码具备分钟级时效性，且时效性具备动态调整能力；

b) 每个用户只可单终端登录，新终端登录旧终端自动下线；

c) 限制二维码连续生码次数，次数可动态配置，超过限制需要验证用户身份合法性；

d) 更换设备登陆，需要验证用户身份的合法性；

e) 二维码应每分钟自动更新；

f) 支付过程中应保证相关设备及系统的安全。

9.7 用户安全

客户端应验证用户的身份，可采用如下方式进行：

a) 用户提供验证信息，例如：客户端密码或口令等；

b) 用户提供所持设备的验证信息，例如：手机动态验证码，令牌等。

10 终端要求

10.1 通用要求

二维码应与刷卡部分分开，二维码扫码隔离直线距离不应少于 6 cm。

应保证在二维码数据图像旋转、不规则变形、图像亮度变化、局部污损等各种复杂情况下准确识读，并具有自动纠错能力。

终端其他要求按照 JT/T 978.3 的规定。

10.2 存储

终端中涉及二维码功能存储容量至少应为256 MB，循环存储至少30000条交易记录.交易记录条数仅为存储的二维码交易记录条数，终端存储的其他要求应符合JT/T 978.3的规定。

生成的交易记录数据在存储器中的存储时间至少为30天。

终端应安全存放机具自身应用程序、发卡机构证书、交易数据、黑白名单等其他参数，确保机具断电数据不丢失。

10.3 通信

终端具备无线通信模块如2G/3G/4G或其他实时联网功能,3G/4G模块要求网络带宽不应小于1024KB，地铁闸机应具备接入局域网功能。

终端应提供对应用程序、机构密钥、参数等数据的下载、更新和删除功能。下载方式可以是本地或远程下载等方式。终端应保证下载的安全控制，只有经过授权或认可方可向终端下载数据，未经授权，不得更改终端中的内容。终端应能够验证下载程序的完整性和正确性，确保敏感数据在下载过程中不会泄漏。

当网络通信模块故障时，终端应支持人工采集上传。

10.4 时钟

终端具备高精度时钟模块，可进行精确授时，应保证正常使用时两次授时期间误差不能大于2 s。

10.5 算法要求

终端应符合GM/T 0003国密算法的规定。

10.6 显示屏

终端的液晶显示屏应支持显示数字、汉字、英文字母等，并能够清楚地向用户展示交易结果，能在高温和低温环境下正常工作，其中汉字显示应符GB/T 2312的规定。

10.7 二维码读取器

10.7.1 一般要求

应支持识别二进制编码格式的二维码，支持识别旋转、倾斜、偏转的二维码，并可通过 USB-HID方式对二维码进行读取。

10.7.2 读取与计算时间

终端完成交通一卡通二维码数据读取至验证成功的处理时间应在300ms内。

10.7.3 识读距离

二维码读取器应能够识别1 cm～10 cm之间展示的二维码。

10.7.4 编码方式

应能够识别QR Code等常用码制。

10.7.5 纠错能力

纠错能力应达到L级（大于等于7%）。

10.8 电源要求

终端应具备断电延时关机功能，保证数据不丢失。

10.9 操作系统要求

应支持 Linux、安卓（Android）等操作系统，其中 Linux 系统中 Glibc 版本应在 2.7 及以上。

10.10 终端监控与管理

应具备远程管理能力，远程监测终端心跳、终端远程进行软件升级、证书下载与更新、黑白名单下载与更新、能远程识别终端问题且具有应急处理的功能。

11 客户端软件要求

11.1 一般要求

客户端应提供包含但不限于以下功能：

a) 保持用户登录会话，提供安全注册，登录，实名验证等功能；
b) 应用软件与后台系统具备合法性检查，通过签名验签等密码技术与后台系统进行双向认证，确保后台系统和应用软件的合法性，并设置超时时间；
c) 若应用软件涉及存储通讯、数据加密的安全密钥，保证客户端每日首次联网时在线更新用户安全密钥的功能；
d) 确保应用程序源代码存储的安全性；
e) 客户端中涉及联机获取的二维码中的敏感数据应采用一定的机制进行分散存储；
f) 对客户端中敏感数据以及涉及处理该数据的程序逻辑进行保护，例如采取代码混淆、加壳、加密等方式，防范攻击者对客户端进行静态分析、逆向工程、调试；
g) 从木马病毒防范、信息加密保护、运行环境可信等方面提升安全防控能力。
h) 用户风险操作提示功能。

11.2 存储

客户端应保障用户公私钥、机构授权数据等信息安全，可采用敏感数据分段存储，且手机客户端程序应保证分段数据组合过程的编程逻辑的安全性。

11.3 显示

客户端应支持显示二维码，并在显示二维码时保持屏幕高亮、常亮，且具有防截屏等功能。

11.4 时钟同步

客户端应定期进行时钟同步，确保与时钟服务器保持同步。

11.5 数据有效性

客户端需提供数据有效性校验功能，应保证通过人机接口或通信接口输入的数据格式符合系统设定要求，如用户名称，身份信息，联系方式等。

11.6 清除敏感信息

客户端在用户确认清除个人敏感数据的情况下，提供清除个人信息的安全机制，避免用户信息泄露。

11.7 反编译

客户端宜采用防逆向工程保护措施，如客户端可采取代码花指令、反调试、代码混淆等技术手段，

防范攻击者对客户端的反编译分析。

11.8 客户端软件完整性

应对客户端程序进行签名，标识客户端程序的来源和发布者，保证客户所下载的客户端程序来源于所信任的机构。

客户端启动和更新时，宜进行真实性和完整性校验，防范客户端被篡改。

11.9 运行安全性

客户端应从木马病毒防范、信息加密保护、运行环境可信等方面提升安全防控能力，并可以通过客户端推送，消息触达等方式，提示用户。

客户端应提供客户端运行环境安状况检测功能，并可以向后台系统反馈客户端软件环境安全状况。

11.10 通信要求

11.10.1 网络通讯协议

客户端与服务器间应建立安全的信息传输通道，通过公开网络进行数据传输时，应通过安全协议传输，如 SSL/TLS 等；

11.10.2 数据传输

通过客户端发送的报文的关键要素宜进行数字签名，以确保关键要素的真实性和抗抵赖性。

12 检测项目

12.1 终端安全

二维码终端安全检测项目见表 18。

表18 二维码终端安全检测项目

序号	检测项目	检测项目说明
1	二维码信息安全	数据解析过程应对二维码中数据信息的完整性、真实性、不可抵赖性及时效性进行鉴别，对于未通过鉴别等非法二维码应予以阻止。
2	账户信息安全	账户信息不应在任何设备和系统中存储。
3	传输信息安全	公网环境下，二维码信息不应以明文形式传输，在传输过程中不被泄露、窃取和篡改。
4	二维码数据生成/解析安全要求	二维码应用于支付环节时应包含可供验证二维码来源合法性的信息，可采用包括但不限于数字签名、合法来源白名单等机制。解码时，应根据对应机制验证二维码来源合法性，确保二维码中不含有木马、病毒和非法链接等有害信息，并应对非法二维码予以明确提示后拒绝交易。
5	用户安全鉴别要求	二维码支付业务的使用者应具备唯一的身份标识，保证对二维码支付的操作能够被追溯到用户。
6		应严格限制使用初始密码，对密码复杂度进行校验，避免采用简单密码或与客户个人信息相似度过高的密码。
7	应用软件安全要求	应具有扫恶意代码（启动木马、转恶意网址等）不跳转或不启动恶意软件等功能。

表 18（续）

序号	检测项目	检测项目说明
8	应用软件安全要求	应用软件程序应从木马病毒防范、信息加密保护、运行环境可信等方面提升安全防控能力。
9		交易过程中，应提供安全提示机制，确保交易过程中关键环节（如：交易金额及交易类型确认，密码输入等）及交易结果能安全、有效向用户提示，用户确认后才可进行下一步操作。
10		应用软件程序应具有抗逆向分析、抗反汇编等安全性防护措施，防范攻击者对客户端程序的调试、分析和篡改；
11		应用软件程序的临时文件中不应出现账户信息，临时文件包括但不限于Cookies；
12		应用软件程序应禁止在身份认证结束后明文存储账户信息，防止账户信息泄露；
13	二维码识读/显示设备安全要求	二维码识读设备和系统应能抵御重放攻击，防止加密数据和交易报文被重用。
14		二维码识读设备固件和应用程序应由收单机构或其授权的生产、维护企业进行签名，设备应对下载的程序文件签名进行合法性验证。
15		受理终端应具备唯一的标识编码，能够通过标识编码追溯到参与交易的受理终端设备。交易报文中应包含受理终端标识编码，并采用技术加密措施和管理措施保证终端标识编码在交易过程中不可被篡改；

12.2 客户端软件

二维码客户端软件安全检测项目见表 19。

表19 二维码客户端软件全检测项目

序号	检测项目	检测项目说明
1	软件自身安全	下载、安装与更新
2		应用软件自检
3		合法性认证和风险控制
4		审计功能
5	用户安全鉴别	用户标识
6		一般用户校验机制
7		双因素验证机制
8		重验证机制

表 19（续）

序号	检测项目	检测项目说明	
9	用户安全鉴别	验证信息保护	
10		失败的验证	
11	账户信息保护	账户信息存储	
12		账户信息输入	
13		账户信息传输	
14		残余信息保护	
15		回退	
16	通信安全	完整性	
17		保密性	
18		原发抗抵赖	
19		接受抗抵赖	
20		网络传输基本要求	
21		网络安全指南和安全评估	
22		实体间通信安全	
23	加密安全	数据加解密	
24		密钥加解密	
25		消息摘要	
26		数字签名	
27		数据完整性验证	
28		客户端密钥管理	
29	密码管理	登录密码管理	
30		支付密码管理	
31	防篡改	软件防反编译	
32		交易防篡改	
33	支付认证	实名认证机制	
34		支付认证机制	
35	人机交互安全	登录控制	
36		支付控制	
37		密码管理	
38		认证方式	
39		鉴别失败处理	
40		重鉴别	
41		移动终端交易异常处理	
42	软件安全	程序异常检测	
43		数据有效性校验	
44		程序调用	
45		反编译	
46	数据安全	数据录入	敏感数据显示
47			敏感数据截获
48			数据篡改
49		数据访问	
50		数据存储	敏感数据存储
51			用户身份认证信息存储安全

表 19（续）

序号	检测项目	检测项目说明	
52	数据安全	数据存储	敏感信息显示
53			残留敏感信息保护
54		数据传输	远程数据传输保密性
55			本地数据传输保密性
56			数据传输完整性
57	通信安全	网络通信安全协议	
58		安全认证	
59		抗抵赖	
60	开发与维护	开发环境	
61		编码漏洞	
62		安全补丁	
63		配置管理	
64		质量检测	
65		发布管理	
66	安装与卸载	下载获取	
67		安装注册	
68		卸载清除	
69	文档支持	用户类文档	
70		工程类文档	
71		管理类文档	

附 录 A
（规范性附录）
符号定义

A.1 符号定义基本约定

文件记录格式中出现的符号定义，见表 A.1。

表A.1 符号定义表

符号	定义
a	字母字符，A～Z，a～z，向左靠，右边多余位填空格
b	数据的二进制表示，后跟数字表示位（bit）的个数
B	用于表示变长的二进制数，后跟数字表示二进制数据所占字节（Byte）的个数
C	选填项
n	数值，0～9，右靠，首位有效数字前填零。若表示人民币金额，则最右二位为角、分
p	填充字符，如空格
s	特殊符号
HEX	16 进制数字 0～9、A～Z
an	字母和数字字符，左靠，右边多余位填空格
as	字母和特殊字符，左靠，右边多余位填空格
cn	压缩数字码，即 BCD 码
ns	数字和特殊字符，左靠，右边多余位填空格
ans	字母、数字和特殊字符，左靠，右边多余位填空格
ansb	字母、数字、特殊字符和二进制数，左靠，右边多余位填空格
M	必填项，若此信息为空，则信息报错
MM	月份，01～12
DD	日期，01～31
YY	年份，00～99
hh	时，00～23
mm	分，00～59
ss	秒，00～59
LL	后面跟随数据元的可变长度值，01～99
LLL	后面跟随数据元的可变长度值，001～999
VAR	可变长度数据元

附 录 B
（资料性附录）
TLV 标签示例

B.1 TLV与扫码信息标签代码示例

TLV 与扫码信息标签代码示例如下：
1000 XXXX 2001 YYYY［上车扫码信息］2002 ZZZZ［下车扫码信息］（实际数据无空格）。
示例结构说明如下：

a) 1000-固定标签；
b) XXXX-后续数据总长度；
c) 2001-第 1 个数据标签；
d) YYYY-上车扫码信息数据总长度；
e) 上车扫码信息-上车扫码内容，示例见 A.2；
f) 2002-第 2 个数据标签；
g) ZZZZ-下车扫码信息数据总长度；
h) 下车扫码信息-下车扫码内容，示例见 A.2。

B.2 扫码信息标签代码示例

扫码标签标签代码示例如下：
0000 0001 0 0001 0004 XXXX ……（实际数据无空格）。
示例结构说明如下：

a) 第 1 个数据标签；
b) 第 1 个标签内容的长度；
c) 第 1 个标签数据内容；
d) 第 2 个数据标签；
e) 第 2 个标签内容的长度；
f) XXXX-第 2 个标签数据内容。