交通一卡通二维码支付技术要求

1 范围

本技术要求规定了交通一卡通二维码（以下简称“二维码”）支付的应用场景、系统框架及流程、二维码数据结构、信息接口、安全要求、终端要求、手机客户端要求等。

本技术要求适用于交通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

GM/T 0002 SM4 分组密码算法

GM/T 0003 SM2 椭圆曲线公钥密码算法

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

JT/T 978.6-2015 城市公共交通 IC 卡技术规范 第 6 部分：安全

3 术语和定义

3.1 发码平台

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。

3.2 发卡机构

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。

3.3 收单机构

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、上送的机构。

3.4 手机客户端

指安装在手机上的应用，用来生成二维码的应用软件。

3.5 受理终端

指可以识别和受理本要求中二维码的终端设备。

3.6 公私密钥对

非对称密钥中的公钥和私钥。

3.7 公钥

非对称密钥对中公开的密钥。

3.8 私钥

非对称密钥对中非公开的密钥。

4 符号和缩略语

下列符号和缩略语适用于本文件。

符号	定义
SM2	国家密码管理局于 2010 年 12 月 17 日发布的椭圆曲线公钥密码算法。
https	是以安全为目标的 HTTP 通道
Cn	压缩数字码，即 BCD 码
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
n	数值，0～9，靠右，首位有效数字前填 0.若表示人民币金额，则最右侧两位为角、分
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
M	必用数据元，如此域没内容，信息出错
C	可选数据元
ans	字母、数字和特殊字符，靠左，右边多余位填空格。
an	字母和数字字符，靠左，右边多余位填空格

5 应用场景

二维码是一种通过特定的编码格式来展示信息的方式，本技术要求主要规定了二维码在交通行业中公交、地铁的应用场景。用户是采用被扫模式即用户手机客户端生成进出站二维码，由受理终端进行扫码。

6 系统架构及流程

6.1 交通一卡通二维码支付系统结构

交通一卡通二维码支付系统结构如图 1 所示。

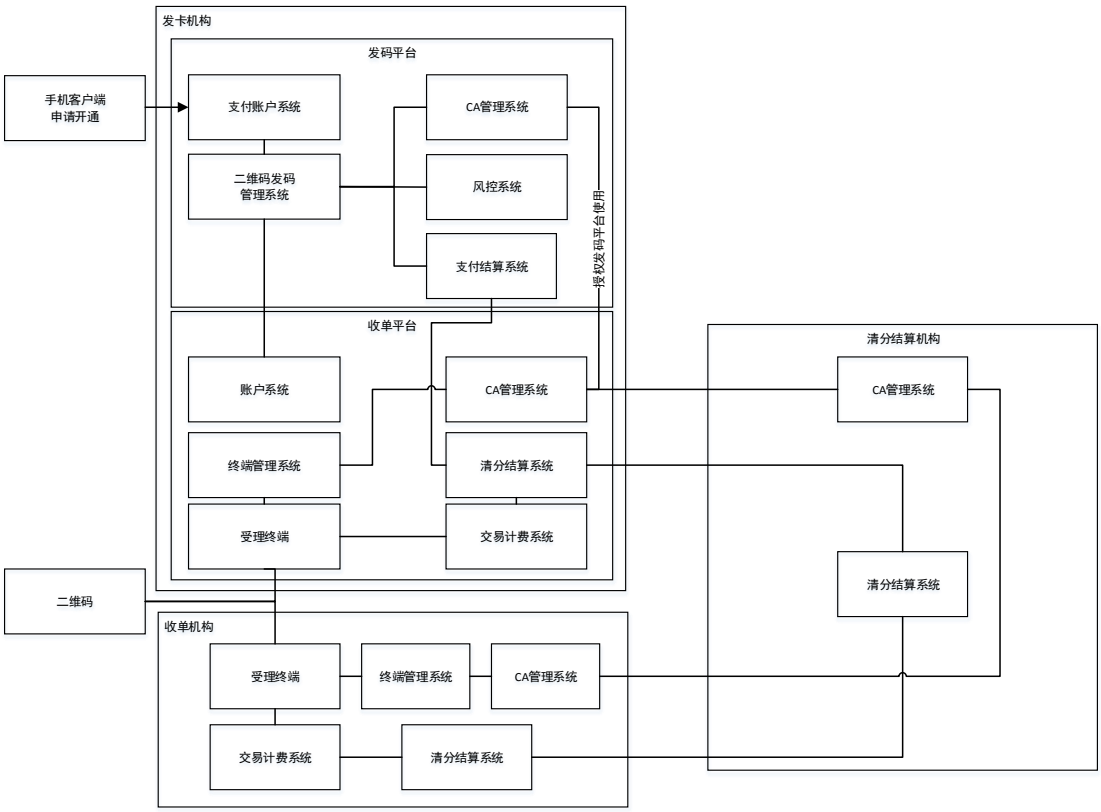


图 1　交通一卡通二维码支付系统结构图

交通一卡通二维码支付系统结构中涉众如下：

a) 清分结算机构的 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) 清分结算系统：负责采集收单机构交易数据、解析交易数据、针对不同入网机构间交易数据进行清分结算以及下发清算文件、对账文件、结算报表等文件；

c) 支付账户系统：负责对二维码消费行为进行记录和管理的系统；

d) 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的管理系统；

e) 发码平台的 CA 管理系统：负责为用户分配公私钥的管理系统；

f) 风控系统：发码机构根据用户交易情况、信用等级等进行风险控制的系统，负责二维码发码安全管理；

g) 支付结算系统：发码机构为发行的二维码消费记录进行支付、结算等资金操作的系统；

h) 发卡机构中收单平台的账户系统：负责管理发卡机构交通一卡通账户、账户消费记录等；

i) 发卡机构的 CA 管理系统：负责与清分结算机构的 CA 系统进行对接，提交申请本机构证书文件、接收清分结算机构下发的入网机构证书、向终端管理系统下发入网机构证书等；

j) 发卡机构/收单机构的清分结算系统：负责与清分结算机构进行对接，上传、下载相关接口文件等；

k) 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；

l) 收单机构的 CA 管理系统：负责与清分结算机构的 CA 管理系统进行对接，接收清分结算机构下发的机构证书，并与本机构终端管理系统进行对接，将机构证书下发至终端管理系统；

m) 终端管理系统：负责下发证书、管理终端软件更新、远程监控终端等；

n) 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。

6.2 交通一卡通二维码支付工作流程

交通一卡通二维码支付工作流程如图 2 所示。

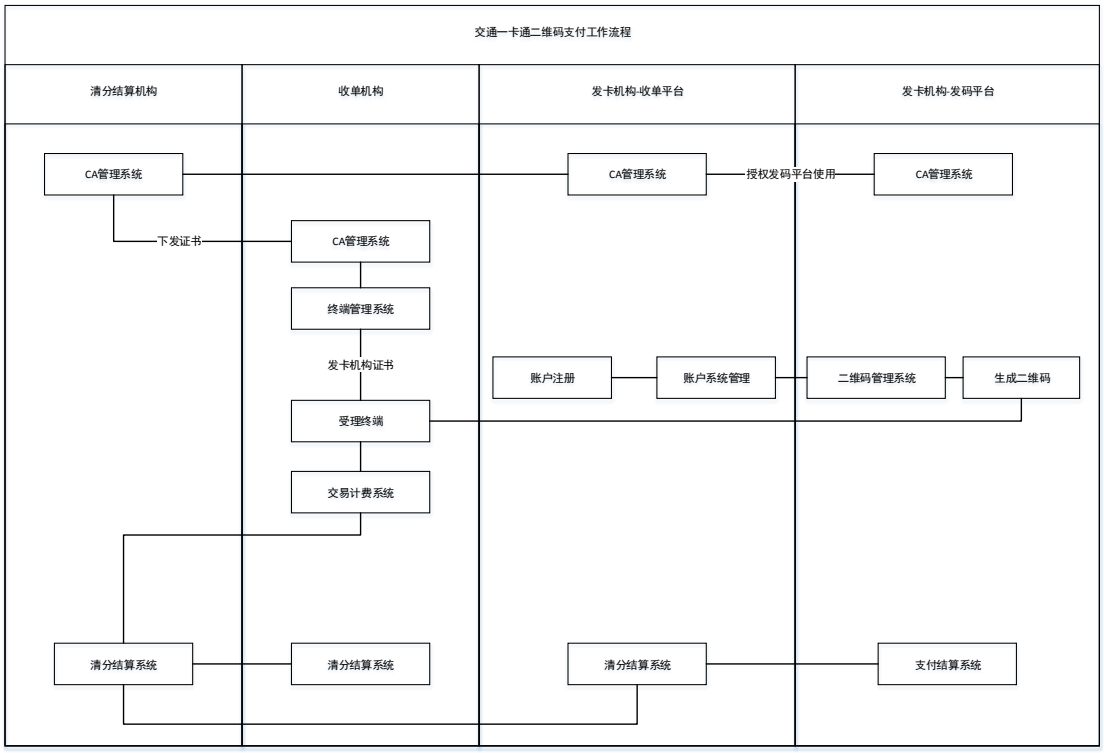


图 2 交通一卡通二维码支付工作流程图

交通一卡通二维码支付工作流程中重点流程说明如下：

a. 参与交通一卡通二维码支付的发卡机构CA管理系统需要定时向清分结算机构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. 清分结算机构的 CA 管理系统应将根公钥下发到收单机构，收单机构负责将中心公钥下发到所有受理终端；

d. 二维码发码平台负责结合账户的信用等级、风险等级等综合因素决定用户可进行预付费交易或信用支付交易，同时，该系统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；

e. 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、完整性，成功识别二维码后将该信息记录并准实时发送至系统后台；

f. 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，最终将统计好的交易数据上传至清分结算机构；

g.清分结算机构的清分结算系统将交易数据转发至账户发行方，并对跨区域交易数据进行清分结算；

h. 发卡机构清分结算系统根据用户消费情况向发码平台进行请款，并完成支付结算。

6.3 交通一卡通二维码支付交易流程

交通一卡通二维码支付交易流程如图 3~5 所示。

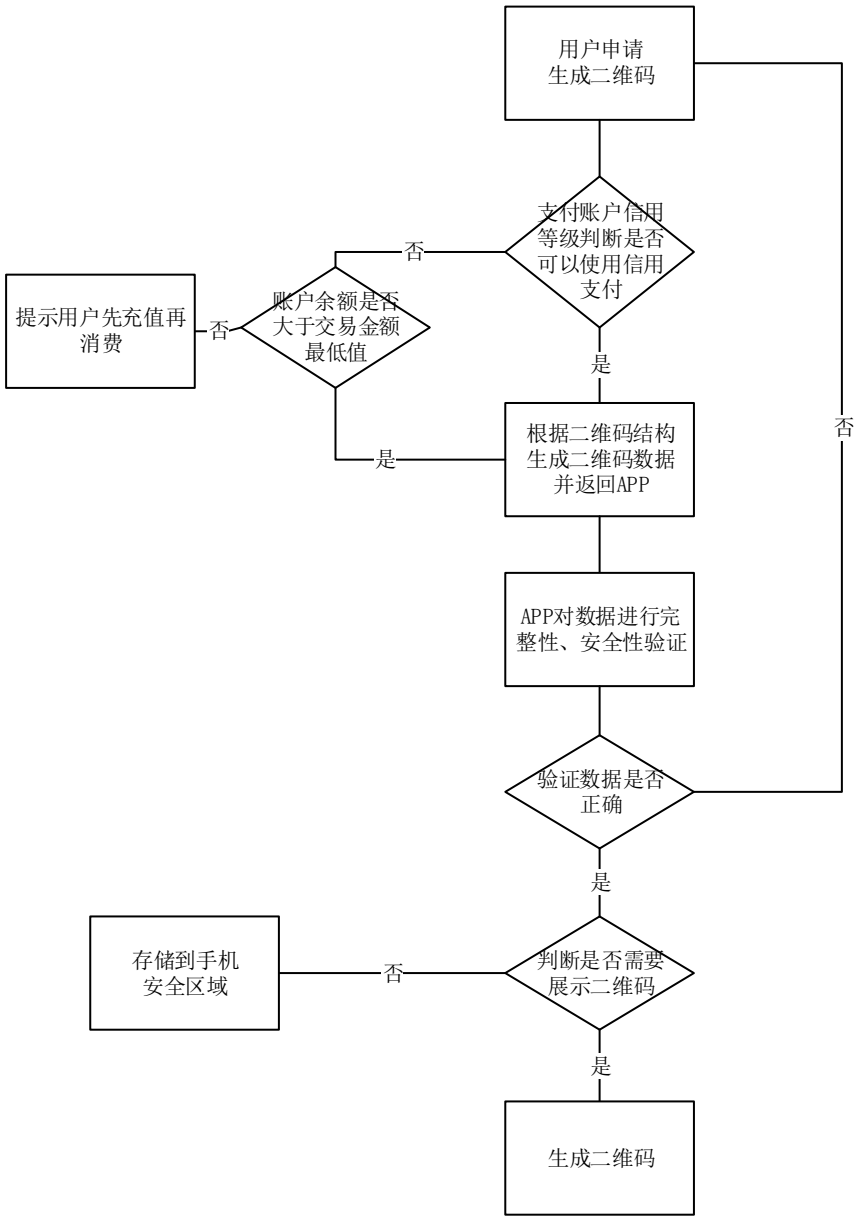


图 3 申请交通一卡通二维码流程图

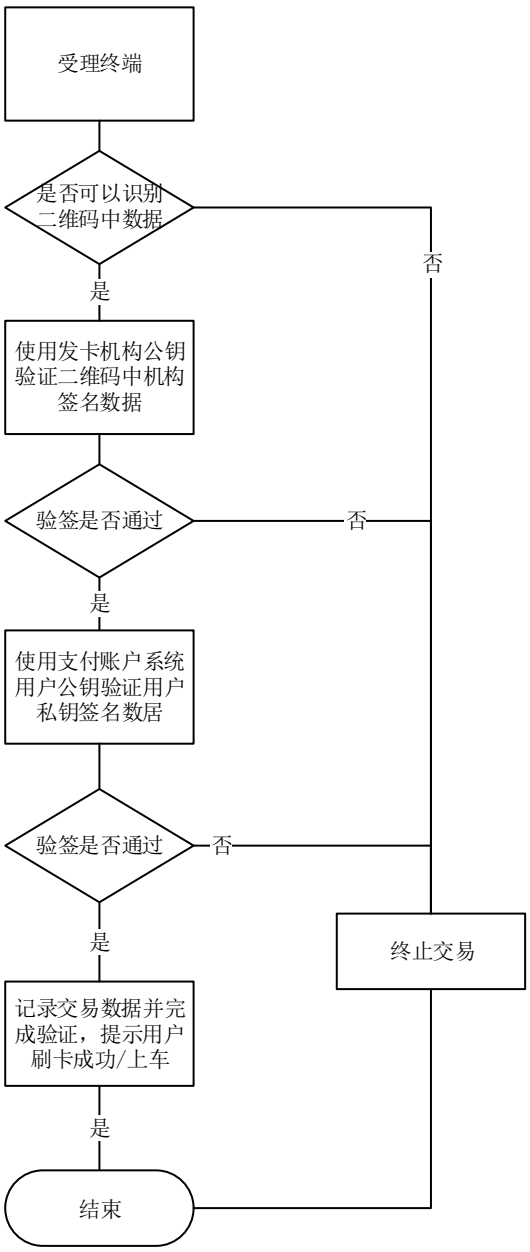


图 4 受理终端识别二维码验证流程图

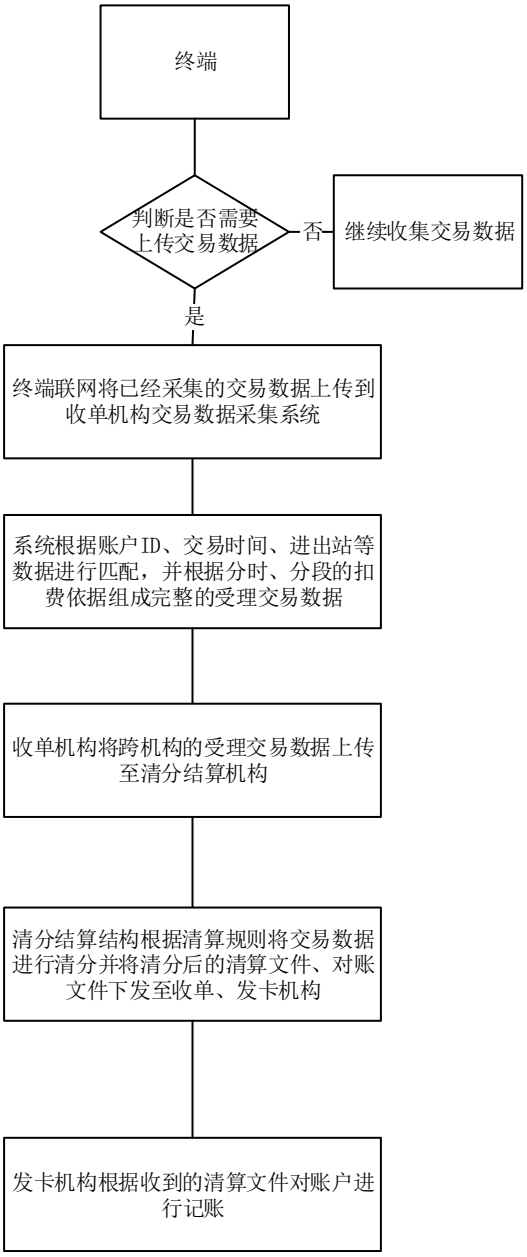


图 5 跨区域交易清分结算流程图

6.4 密钥工作原理

6.4.1 二维码数据加密流程

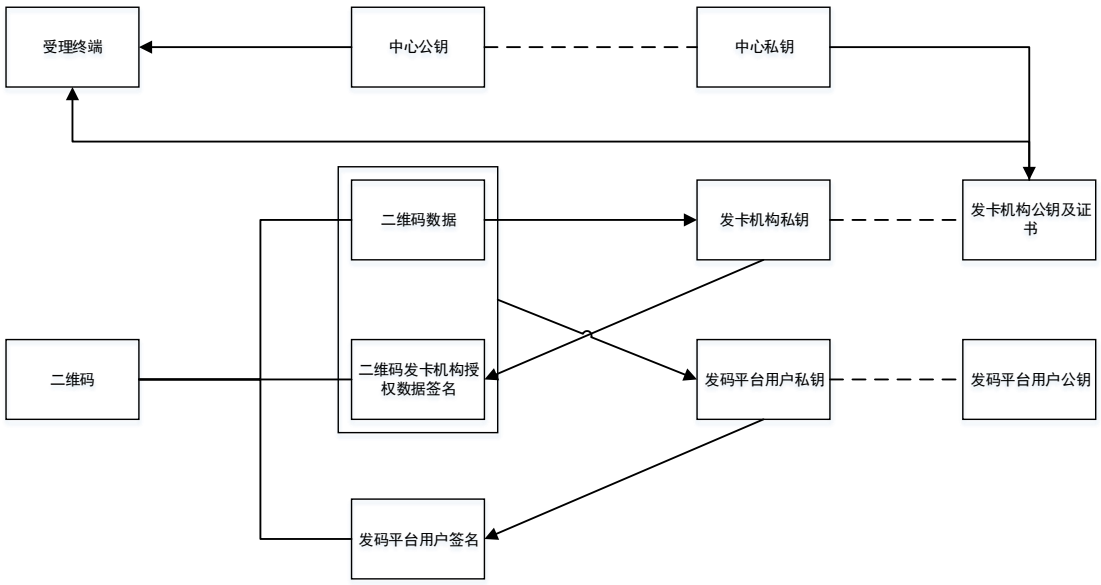
交通一卡通二维码需要使用二级密钥进行保护，包括：发卡机构级和发码平台用户级，工作原理如图所示，其中：

a) 发卡机构公钥证书是使用清分结算机构私钥对发卡机构公钥进行签名生成的证书；

b) 发码平台用户公/私钥是发码平台为其用户分配的独立、不重复的密钥对；

c) 用户密钥可安全存储于手机客户端，此时应保证手机客户端的安全性，并保证秘钥存储的安全性；

d) 用户密钥可存放于支付账户系统中，且应以密文形式存储。



注 1：使用发卡机构私钥对二维码数据进行签名形成二维码发卡机构授权数据签名；

注 2：使用发码平台用户私钥对二维码数据以及二维码发卡机构授权签名数据进行签名形成发码平台用户签名。

图 6 交通一卡通二维码数据安全结构图

6.4.2 受理终端验签流程

受理终端验证二维码的合法性流程如图 7 所示，其中：

a. 受理终端使用发卡机构公钥验证发卡机构授权签名数据的合法性、有效性；

b. 受理终端使用二维码中包含的发码平台用户公钥验证二维码中的发码平台用户签名数据的合法性、有效性。

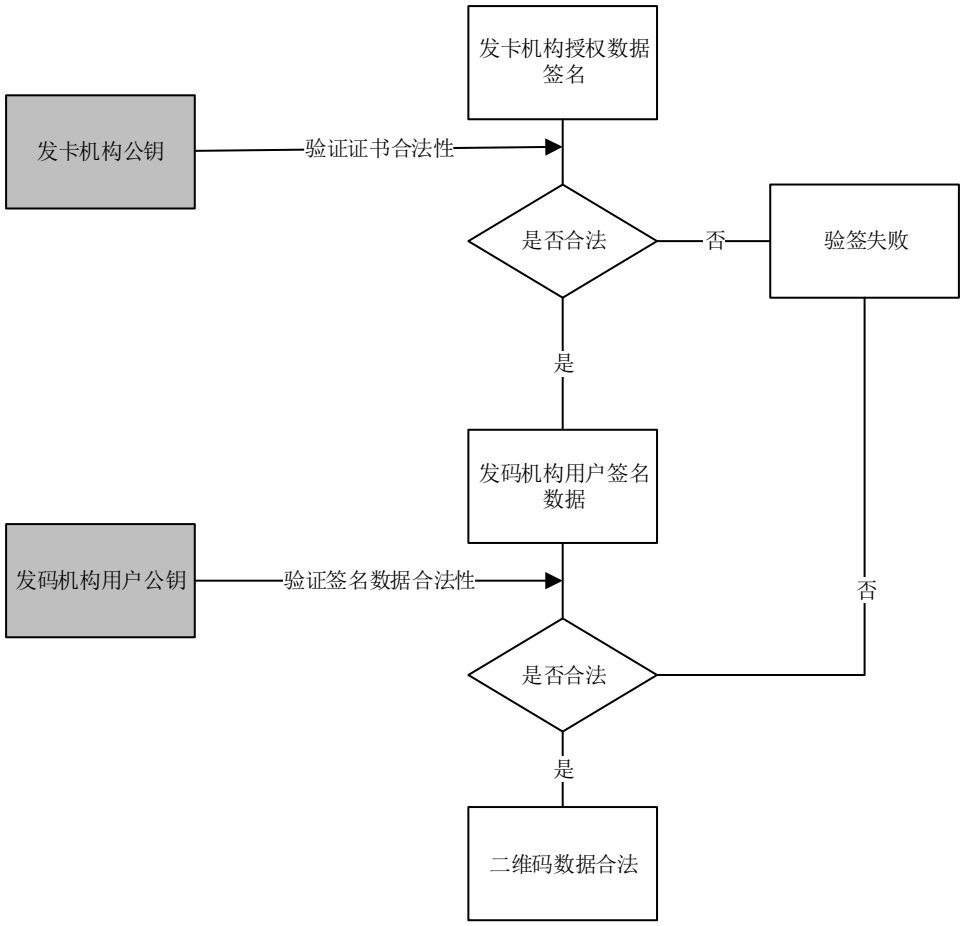


图 7 交通一卡通二维码终端验签流程图

7 交通一卡通二维码数据结构

7.1 编码格式

符合《QRCode 国家标准 GB/T 18284-2000》规范，采用二进制（8bit-byte）编码方式。

7.2 结构定义

7.2.1 交通一卡通二维码结构

交通一卡通二维码结构如图 8 所示。

二维码数据头														
二维码版本号			二维码类型			发码方式			发卡机构证书编号					
1			2			1			4					
二维码数据体														
机构授权数据长度	支付账户号	发卡机构号	发码平台编号	交通一卡通卡号	卡类型	单次消费金额上限	批次号	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	发卡机构授权数据签名	用户授权数据长度	二维码生成时间	支付账户用户私钥签名
2	16	4	4	10	1	3	3	33	4	2	65	2	4	65

图 8 交通一卡通二维码结构图

7.2.2 交通一卡通二维码结构定义

交通一卡通二维码数据结构定义见表 1。

表 1 交通一卡通二维码数据结构表

序号	字段名	字节长度	描述	格式	是否必填
1	二维码版本	1	二维码结构版本号。 0x80~0xFF 交通一卡通二维码标准版本，当前0x80	B	M
2	二维码类型	2	定义二维码的类型： 1) JT00-公交； 2) JT01-地铁； 3) JT02-出租车； 4) JT03-公共自行车； 5) JT04～JT99本要求保留。	Cn4	M
3	发码方式	1	定义发码的方式： 1) 00-联机发码； 2) 01-脱机发码。	B	M
4	发卡机构证书编号	4	发卡机构证书编号，编号在发卡机构向清分结算机构申请证书时分配，发卡机构可申请多份证书，证书编号发卡机构不可随意改动。	B	M
5	发卡机构授权数据长度	2	发卡机构数据长度。	B	M
6	支付账户号	16	由支付账户系统自定义。	ans	M
7	发卡机构号	4	由清分结算机构统一分配。	B	M
8	发码平台编号	4	由清分结算机构统一分配。	B	M
9	交通一卡通卡号	10	同JT/T 978中卡号的要求	B	M
10	卡类型	1	见JT/T 978.2中表A.1中发卡机构特殊数据元	B	M

			第20字节卡种类型。		
11	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。	n	M
12	批次号	3	表示针对当前用户联机下发一组二维码数据的批次。	B	M
13	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 0003.1中A.5。	B	M
14	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	B	M
15	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
16	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5～17字段。	B	M
17	用户授权数据长度	2	用户授权数据长度	B	M
18	二维码生成时间	4	二维码生成时间戳	B	M
19	支付账户用户私钥签名	65	支付账户用户私钥签名数据，此签名是对二维码数据体进行签名。	B	M

总计长度为 226 字节。

7.2.3 数据签名

使用 SM2 算法的签名数据内容见表 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

7.2.4 发卡机构公钥数据

发卡机构公钥数据是发卡机构提供的本机构公钥数据,见表 3。

表 3 发卡机构公钥数据

字段名	长度	描述	格式	是否必填
证书格式	1	十六进制，值为‘14’	b	M
证书失效日期	2	MMYY，在此日期后，这张证书无效	n4	M
证书序列号	3	由发卡机构分配给这张证书的唯一的二进制数	b	M
二维码公钥签名算法标识	1	标识使用在二维码公钥上的数字签名算法。SM2算法为‘04’。	b	M
二维码公钥加密算法标识	1	标识二维码公钥对应的加密算法，暂不使用，取值‘00’。	B	M
二维码公钥参数标识	1	用于标识椭圆曲线，同时确定NIC。见附录A.1	b	M
二维码公钥长度	1	标识二维码公钥的字节长度	b	M
二维码公钥	64	如果二维码公钥算法标识对应于SM2,该字段为椭圆曲线上的一	b	M

		个点 。		

7.2.5 发卡机构公钥和证书

使用 SM2 算法，清分结算机构私钥对 7.2.4 数据进行签名的证书数据格式，本部分总长度为 106 字节，见表 4。

表 4 机构公钥及证书

字段名	长度	描述	格式	是否必填
证书格式	1	十六进制，值为‘14’	B	M
证书失效日期	2	MMYY，在此日期后，这张证书无效	n4	M
证书序列号	3	由发卡机构分配给这张证书的唯一的二进制数	B	M
二维码公钥签名算法标识	1	标识使用在二维码公钥上的数字签名算法。SM2算法为‘04’。	B	M
二维码公钥加密算法标识	1	标识使用在二维码公钥上的加密算法，暂不使用，取值‘00’。	B	M
二维码公钥参数标识	1	用于标识所用的椭圆曲线。见附录A.1	B	M
二维码公钥长度	1	标识二维码公钥的字节长度	B	M
二维码公钥	64	32位X轴曲线，终端根据X轴曲线计算出Y轴曲线，合成XY椭圆曲线。	B	M
数字签名	64	发卡机构对表2数据计算的SM2签名r||s	B	M

7.2.6 算法与密钥

本技术要求中清分结算机构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公钥 X 轴数据计算 Y 轴数据时使用的算法应符合 GM/T 0003 的规定。

8 信息接口

8.1 一般要求

交易记录是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的，且已计算出乘车消费金额的交易记录，收单机构需要将此记录上传至中心的清分结算系统，清分结算系统根据清算规则对交易记录进行清分结算，并将清分结算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。

8.2 文件类型

文件类型包括交易类接口和清算类接口见表 5。

表 5 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。

8.3 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详见 JT/T 978.4-2015 中 7.3 节。发卡机构、收单机构与清分结算系统间报文交换流程见图 9 和图 10。

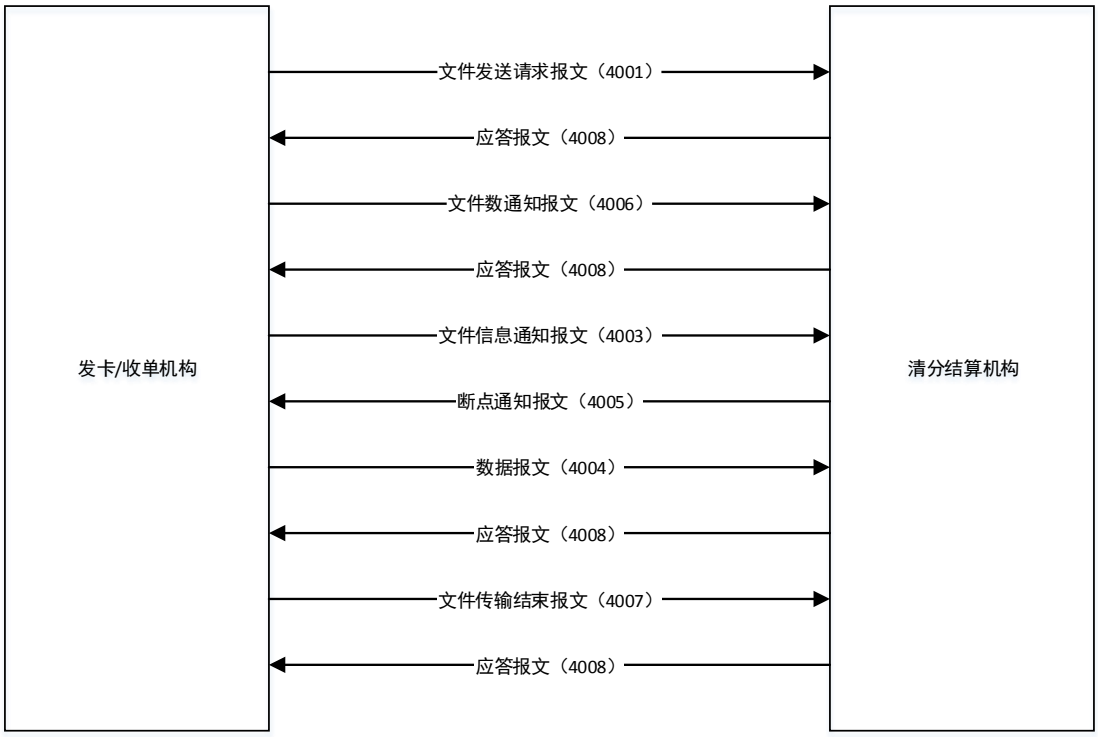


图 9 上传文件交互流程图

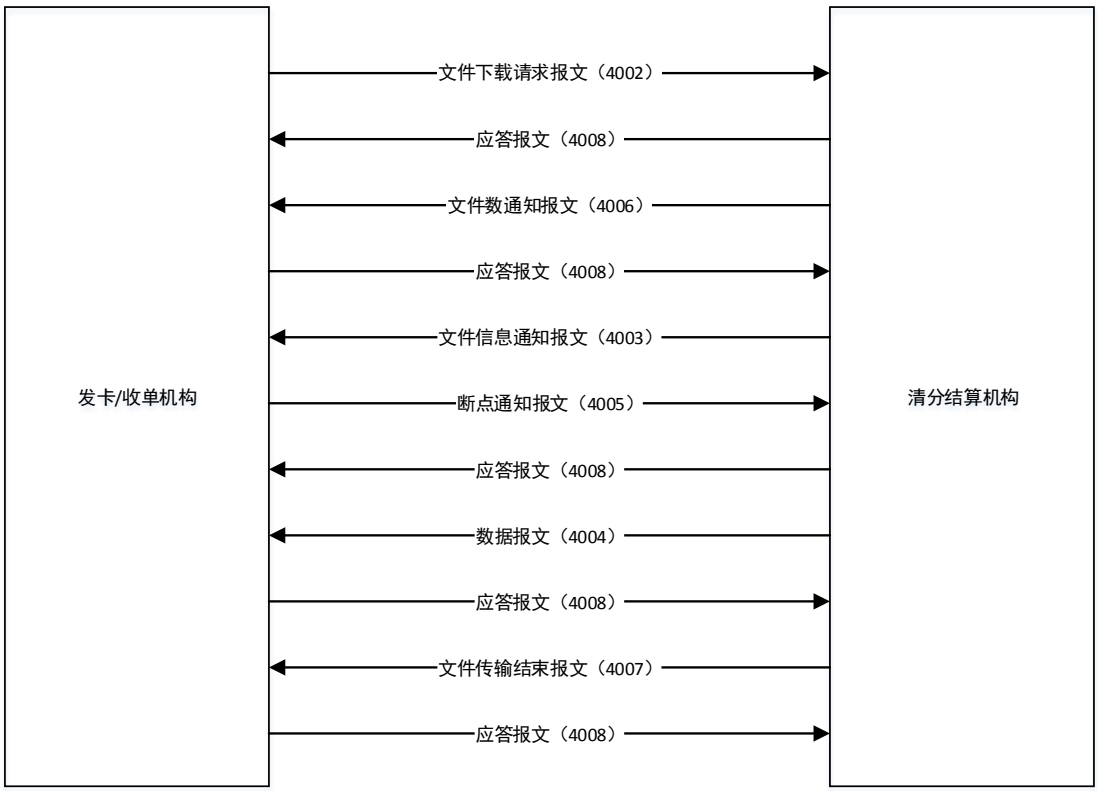


图 10 下载文件交互流程图

8.4 交易记录文件命名规则

交易记录文件命名规则见表 6。

表 6 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	4	BCPD/BCPR
日期	n	24	年份用后两位，YYMMDDhhmmss
机构代码	n	16	清分结算机构分配
序列号	ans	20	机构自定义
文件标志	an	2	H-手工账，A-自动账

8.5 交易记录文件结构

交易记录文件采用顺序文件结构，且以流文件的方式进行传输。顺序文件结构见 JT/T 978.4-2015 中 6.1.3。

8.6 交易记录结构

交易记录文件是由交易记录头、交易记录体和交易记录尾组成。

8.6.1 交易记录头

交易记录头内容见表 7。

表 7 交易记录头

字段名	长度	描述	格式	是否必填	说明
开始标志	5	标志记录头的开始。	an	M	由发送方填写，内容为JTPAY
交易总笔数	4	交易记录文件中包含的交易记录笔数，不包含记录头和记录尾	n	M	由发送方填写。
交易总金额	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	由发送方填写。交易记录文件中包含的交易记录的总金额。
版本标记	4	版本标记（TEST/PROD）	an		只填写TEST或PROD a） TEST-测试版本； b） PROD-生产版本。
版本号	8	版本号	an	M	版本号为00000001

8.6.2 交易记录尾

交易记录尾内容见表 8。

表 8 交易记录尾

字段名	长度	描述	格式	是否必填	说明
版本标记	4	版本标记（TEST/PROD）	an		只填写TEST或PROD c） TEST-测试版本； d） PROD-生产版本。
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。

8.6.3 交易记录体

交易记录数据结构见表 9。

表 9 交易记录数据格式

字段名	长度	内容	格式	是否必填	说明
记录长度	2	本条交易记录总长度	B	M	
交易类型	4	见表 1 中二维码类型。	Cn	M	
消费类型	2	消费类型	n	M	消费类型： 00-表示单次消费； 01-表示复合消费。
扫码类型	2	扫码类型	n	M	扫码类型：

字段名	长度	内容	格式	是否必填	说明
					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	6 位定长数字字符，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	
支付账户号	16	主账号	Cn	M	在右边补上十六进制数‘F’
收单机构号	4	收单机构标志码。	n	M	
发卡机构号	4	发卡机构标志码。	n	M	
发码平台编号	4	发码平台标志码。	n	M	
商户类型	4	收单机构商户类型吗[表示商户分类编码（MCC）]	n	M	
进站二维码长度	2	进站二维码数据总长度	B	C	当扫码类型为 01 时，任意消费类型均需填写此域。
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	
货币代码	3	交易币种	an	M	人民币 CNY
进站二维码内容	259	进站二维码数据内容	B	C	当扫码类型为 01 时，任意消费类型均需填写此域。
出站二维码长度	2	出站二维码数据总长度		C	当扫码类型为 01 且消费类型为 01 时，则此域必填。
出站二维码内容	259	出站二维码数据内容	B	C	当扫码类型为 01 且消费类型为 01 时，则此域必填。
进站终端 ID	8	同 JT/T 978 中终端编号的要求。	ans	M	
出站终端 ID	8	同 JT/T 978 中终端编号的要求。	ans	M	
进站时间	14	二维码用户进站时间。格式为 YYYYMMDDhhmmss	n	M	
出站时间	14	二维码用户出站时间。格式为 YYYYMMDDhhmmss	n	M	

字段名	长度	内容	格式	是否必填	说明
检索参考号	n	12	取值范围000000000001～999999999999		

8.7 FB 二维码交易清算反馈文件

8.7.1 用途

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。

8.7.2 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	01
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	666-二维码支付
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
渠道类型	an	2	04-二维码扫码POS机
交通一卡通卡号	n	20	16位～19位。 不足右补空格
卡消费计数器	n	6	填充000000
交易金额	n	12	取值范围000000000001～999999999999
交易日期	n	8	YYYYMMDD
交易时间	n	6	HHMMSS

算法标识（也加到FB文件中）	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	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
预留字段	ans	28	
保留域	ans	40	全F
回车符	s	2	0x0D和0x0A

8.8 CL 二维码交易清算明细文件

8.8.1 用途

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。

8.8.2 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	01
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	666-二维码支付
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
发卡机构清算机构代码	n	11	右补空格，交易发生地单位
发卡机构代码	n	11	右补空格，发卡地
MCC	an	4	参考MCC文档
渠道类型	an	2	04-二维码扫码POS机
交通一卡通卡号	n	20	16位到19位 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000000000001～999999999999
交易日期	n	8	YYYYMMDD
交易时间	n	6	hhmmss
算法标识	an	2	d) 01-3des e) 02-SM2 f) 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

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
预留字段	ans	28	
回车符	s	2	0x0D和0x0A

9 安全要求

9.1 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，例如：私钥应存储在手机安全区域如 SE、TEE 等，防止信息泄露和篡改。

9.2 通信安全

9.2.1 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，确保数据不对监听和篡改，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。

9.2.2 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完整性的校验。

9.2.3 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。

9.3 应用软件安全

9.3.1 合法性检查和风险控制

应用软件与后台系统应具备合法性检查，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。

9.3.2 密钥更新要求

若应用软件涉及存储通讯、数据加密的安全密钥，应保证密钥定期更新，以防密钥丢失。

9.3.3 应用软件安全

应用软件应保证如下要求：

a. 应确保应用程序源代码存储的安全性，即应用程序源代码不可泄露；
b. 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。
c. 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；
d. 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。

9.3.4 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，并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安全。

9.3.5 用户安全

客户端应验证用户的身份，可采用如下方式进行验证：

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，例如：手机动态验证码，令牌等；

10 终端要求

10.1 通用要求

二维码与刷卡部分必须分开，需要刷卡在上、二维码在下。二维码扫码隔离直线距离不少 6 厘米。

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，可准确识读，并具有较强的自动纠错能力。

终端其他要求见 JT/T 978.3。

10.2 存储

终端应保证至少存储 1000 张机构证书，存储至少 500 条交易记录。

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、黑白名单等其它参数，并确保机具断电这些数据不丢失。

10.3 通信

具备无线通信模块如 2G/3G/4G，如果是地铁闸机应具备 WLAN 端口，支持接入局域网、互联网，并支持二维码机构密钥更新下载。

终端应能够准实时将用户扫码行为同步到服务器端。

10.4 时钟

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

10.5 算法要求

应符合 GM/T 0003 国密算法的规定。

10.6 二维码读取器

10.6.1 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，并可以通过 USB-HID 方式对二维码进行读取。

10.6.2 读取与计算时间

应在 200ms 内完成二维码读取与验证。

10.6.3 编码方式

应 QR Code 等常用码制。

10.6.4 读取精确度

可支持识别旋转、倾斜、偏转的二维码。

10.7 操作系统要求

应支持 Linux 操作系统，且 Linux 系统中 glibc 版本应在 2.7 及以上。

10.8 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、机构证书下载与更新、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能力。

11 手机客户端要求

11.1 存储

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。

11.2 显示

支持显示二维码，并在显示二维码时保持屏幕高亮、常亮，并做到防截屏等功能。

11.3 时钟模块

手机客户端应定期进行时钟同步，确保与时钟服务器保持同步。

附录 A

(规范性附录)

椭圆曲线标识

A.1　椭圆曲线标志

椭圆曲线标识见表 A.1。

表 A.1 椭圆曲线标识

算法类型	强度	曲线	公钥长度	曲线标识
ECC	128 位	NIST P-256	64 字节	“01”
ECC	256 位	NIST P-521	132 字节	“02”
SM2	128 位	SM2	64 字节	“11”