ICS 03.220.20
CCS R 07

DB44

广 东 省 地 方 标 准

DB44/T 2310—2021

城市公共交通二维码应用技术规范

Technical Specification for Two-Dimensional Code in Guangdong's Municipal Public Transportation

2021－06－13 发布　　2021－09－13 实施

广东省市场监督管理局　　发 布

目　　次

前言 II
1　范围 1
2　规范性引用文件 1
3　术语和定义 1
4　缩略语 1
5　系统架构 2
6　二维码数据格式 3
6.1　编码格式 3
6.2　数据结构 3
6.3　发码机构自定义域定义和说明 5
6.4　交通行业自定义说明 5
7　信息接口 5
7.1　说明 5
7.2　交互协议 6
8　受理终端要求 11
9　客户端软件要求 11
10　安全规范 11
附录A（规范性）　符号定义表 12

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由广东省交通运输厅提出，并组织实施。

本文件由广东省交通运输（公路水路）标准化技术委员会（GD/TC　133）归口。

本文件起草单位：广东岭南通股份有限公司、广州羊城通有限公司、广东省道路运输事务中心、广州市公共交通数据管理中心、深圳市腾讯计算机系统有限公司。

本文件主要起草人：谢振东、方秋水、易智君、何建兵、刘兵、袁勇、徐锋、吴金成、温晓丽、于航、曾江、程世勇、郭贵城、陈历军。

广东省城市公共交通二维码应用技术规范

1 范围

本文件规定了广东省城市公共交通领域二维码应用的数据格式、安全性、服务器数据交换协议、受理终端以及客户端软件的要求。

本文件适用于广东省城市公共交通二维码的服务系统、终端、客户端软件等的设计、研发与应用。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 2312 信息交换用汉字编码字符集 基本集

GB/T 18284—2000 快速响应矩阵码

GB/T 32918（所有部分） 信息安全技术 SM2椭圆曲线公钥密码算法

JT/T 978.3 城市公共交通IC卡技术规范 第3部分：读写终端

JT/T 1179—2018 交通一卡通二维码支付技术规范

3 术语和定义

JT/T 1179—2018界定的以及下列术语和定义适用于本文件。

3.1

城市公共交通 municipal public transportation

运用公共汽电车、城市轨道交通、城市客运轮渡等运载工具和有关设施，按照核定的线路、站点、时间、票价运营，为公众提供基本出行服务的城市客运方式。

4 缩略语

下列缩略语适用于本文件。

3DES：三重数据加密算法（Triple DES）

CA：电子商务认证授权机构(Certificate Authority)

FTP：文件传输协议(File Transfer Protocol)

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

MAC：消息认证码（Message Authentication Code）

MAK：MAC密钥(MAC Key)

MD5：信息—摘要算法（message—digest algorithm 5）

MMK：成员主密钥(Member Master Key)

QR CODE：快速响应矩阵码（Quick Response Code）

RSA：一种非对称加解密技术（Rivest Shamir Adleman）

SM2：SM2椭圆曲线公钥密码算法(Public Key Cryptographic Algorithm SM2 Based on Elliptic Curves)

SM3：SM3密码杂凑算法(SM3 Cryptographic Hash Algorithm)

SM4：SM4分组密码加密算法(SM4 Cryptographic Algorithm)

SSL/TLS：安全套接层/传输层安全(Secure Sockets Layer/Transport Layer Security)

TLV：标签、长度、值(Tag Length Value)

TAC：交易认证码（(Transaction Authentication Code）

UID：用户账户标识（User Account Identifier）

UIID：用户账户发行方标识（User Account Issuer Identity）

UTC：协调世界时(Coordinated Universal Time)

5 系统架构

广东省城市公共交通二维码应用系统由省级清算管理机构、发码机构、收单机构、受理终端、客户端软件组成。系统架构见图1。

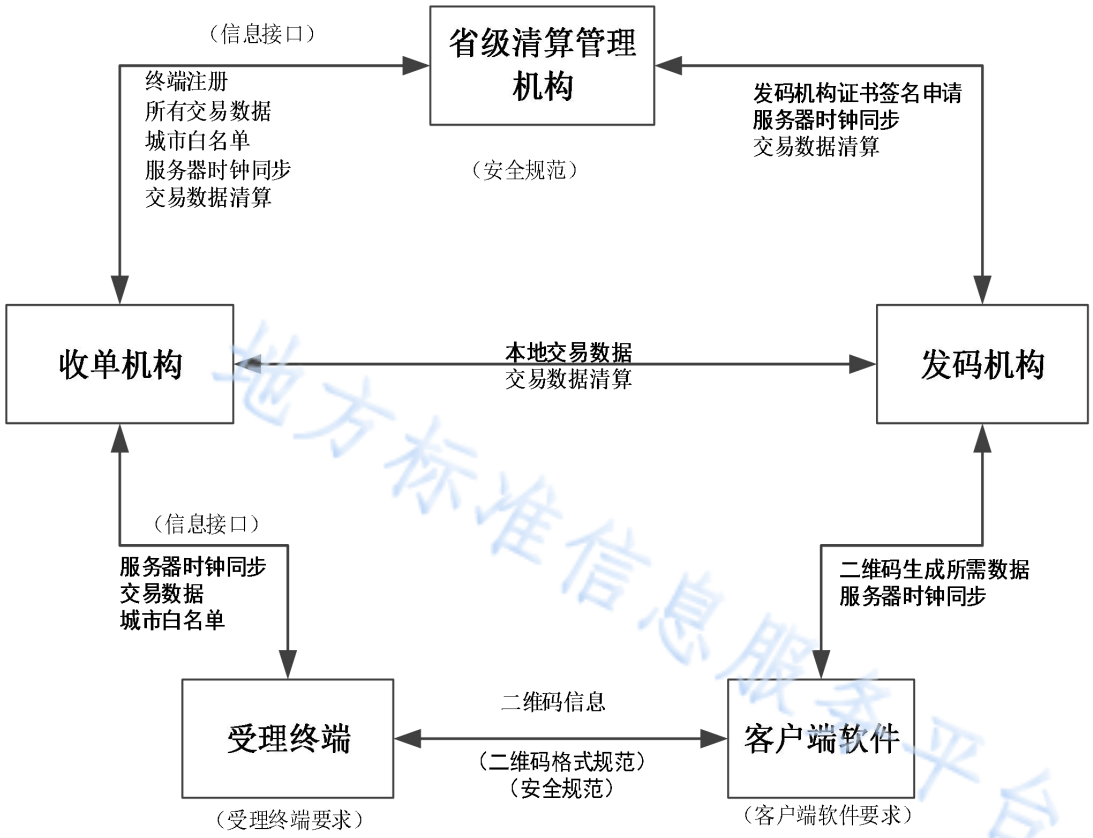

图 1 系统架构示意图

省级清算管理机构：省级二维码清结算业务运营主体，负责全省二维码交易数据的归集，以及负责省内跨城市、跨机构之间的二维码交易清分与结算，负责发码机构证书的统一申领和发放，负责各发码

机构互联互通的配置管理，发码机构、收单机构、受理终端、客户端软件的时间均同步省级清算管理机构服务器的时间。

发码机构：城市公共交通二维码运营主体或其它二维码运营主体，负责用户管理、资金渠道管理、二维码密钥服务、城市二维码数据清结算及交易风险控制。发码机构申请二维码流程、受理终端验证二维码流程、跨区域交易清分结算流程应符合JT/T 1179—2018的要求。

收单机构：城市公共交通二维码交易终端运营主体或其它二维码交易终端运营主体，负责受理终端安装、系统维护、交易数据采集和上传。

受理终端：用于二维码交易的终端设备。扫码方式采用受理终端主扫模式。

客户端软件：用于生成二维码的应用程序，包括用户注册、用户登录、密钥申请以及二维码生成等功能。

6 二维码数据格式

6.1 编码格式

二维码的编码格式应符合JT/T 1179—2018的要求。

6.2 数据结构

二维码数据主要由17个字段组成，包括：二维码版本、二维码数据长度、城市发码机构公钥证书、支付账户号、用户账户号、城市发码机构代码、发码平台代码、用户账户类型、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、城市发码机构自定义域长度、城市发码机构自定域、城市发码机构授权签名、二维码生成时间和支付账户用户私钥签名。二维码数据结构见表1，二维码数据结构说明见表2，二维码数据结构说明中出现的格式符号要求见附录A。

表 1 二维码数据结构

二维码结构															
二维码版本	二维码数据长度	城市发码机构公钥证书	支付账户号	用户账户号	城市发码机构代码	发码平台代码	用户账户类型	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	城市发码机构自定义域长度	城市发码机构自定域	城市发码机构授权签名	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	1	32	65	4	65

表 2　二维码数据结构说明

序号	字段名称	长度	格式	必填	字段说明
1	二维码版本	1	B	M	范围为 0x80—0xFF
2	二维码数据长度	2	B	M	固定长度为 0x016C
3	城市发码机构公钥证书	117	B	M	应符合 JT/T　1179—2018 第 9 章的要求
4	支付账户号	16	ans	M	由支付账户系统自定义，长度不足前补“0”
5	用户账户号	10	B	M	由城市发码机构账户管理平台定义，长度不足前补“0”
6	城市发码机构代码	4	B	M	由清算机构统一分配
7	发码平台编码	4	B	M	由清算机构统一分配
8	用户账户类型	1	B	M	用户账户的类型(默认为 0x01) 0x01:普通卡 0x02：学生卡 0x03：老人卡 0x04：测试卡 0x05：军人卡 其他：城市发码机构自定义
9	单次消费金额上限	3	B	M	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
10	用户公钥	33	B	M	经过压缩的支付账户系统中用户公钥数据，压缩方法应符合 GB/T　32918 的要求
11	系统授权过期时间	4	B	M	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 到当前的秒数，高字节在前
12	二维码有效时间	2	B	M	以秒为单位，此域在填写时无须带单位，高字节在前
13	城市发码机构自定义域长度	1	B	M	城市发码机构自定义域数据长度为 32
14	城市发码机构自定义域	32	B	M	城市发码机构自定义，由城市发码机构自定义域，格式见 6.3
15	城市发码机构授权签名	65	B	M	城市发码机构私钥签名，签名数据包括本表中序号为 3—14 字段，应符合 JT/T　1179—2018 的要求
16	二维码生成时间	4	B	M	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　到当前的秒数，高字节在前
17	支付账户用户私钥签名	65	B	M	支付账户用户私钥签名数据，签名数据包括本表序号为 1—16 字段，应符合 JT/T　1179—2018 的要求

6.3 发码机构自定义域定义和说明

发码机构自定义数据结构见表3。

表 3 发码机构自定义数据结构

序号	名称	长度	格式	标签说明
1	发码机构保留区域	11	B	由发码机构定义
2	交通行业类型标识	1	B	01：公交 02：城市轨道 03：轮渡 04：出租车 05：城际轨道 06：道路客运
3	交通行业自定义数据	20	B	见 6.4

6.4 交通行业自定义说明

发码机构自定义数据结构见表4。

表 4 发码机构自定义数据结构

序号	交通行业类型标识	标签说明
1	02	第 1 字节为乘车码验证方式，0x1 脱机验证；0x2 联网验证；0x3 连防重系统验证 第 2—3 字节为流水号，每次交易里程使用一个流水号 第 4 字节为车票状态，0x1 初始状态；0x2 已进站；0x3 已出站；0x4 进站更新状态；0x5 出站更新状态 第 5—6 字节为车站编码，上一次处理车票的车站编码，由线路和站点组成 第 7—10 字节为车票处理时间，上一次处理车票的时间 第 11—14 字节为行业数据过期时间 第 15—18 字节为地铁后台账户 ID 第 19—20 字节为在线自助更新站点
2	其他	保留

7 信息接口

7.1 说明

7.1.1 通讯方式

通讯方式应使用HTTPS协议，POST请求数据方法。

7.1.2 数据交换格式

数据交换格式为JSON（JavaScript Object Notation）。

7.1.3 接口数据签名

应对数据进行数字签名，在接收签名数据之后进行签名校验。

数字签名有两个步骤，先按7.1.4规则拼接签名原始串，再选择7.1.5的算法和密钥计算出签名结果。

7.1.4 签名原始串

签名原始串应按以下方式组装成字符串：

——除签名字段外，所有参数按照第一个字符的键值 ASCII 码递增排序，遇到相同字符则按照第二个字符的键值 ASCII 码递增排序，以此类推；

——排序后的参数与其对应值组合成“参数名=参数值”的格式，并用“&”字符连接起来。签名原始串中，参数名和参数值都采用原始值。

7.1.5 签名算法

对签名原始串的尾部加上字符串“&key=”，再加上签名密钥值，形成待签名字符串，使用MD5算法，对待签名字符串计算MD5值，再转成大写字符串。

示例：

JSON数据中有3个参数，其表达为：{”service”:”abc”,”timestamp”:”123”,”version”:”1.0”}。

签名原始串示例为：service=abc&timeStamp=123&version=1.0

签名密钥值为：123456

签名字符串示例为：service=abc&timeStamp=123&version=1.0&key=123456

签名字符串的MD5值为：88046c2fa808dc6c71a6ee3eb7c9b812

签名字符串的MD5值转换为大写为：88046C2FA808DC6C71A6EE3EB7C9B812

7.2 交互协议

7.2.1 公共参数

接口协议中的请求报文必须包含请求公共参数的所有字段见表5，接口协议中应答报文必须包含应答公共参数见表6。

表 5　请求公共参数

序号	字段名	参数名	长度	类型	说明
1	接口版本	version	<=20	字符串	例如“1.0”
2	接口名称	service	<=50	字符串	见各接口说明 例如“TermRegist”
3	通道编号	channelCode	8	字符串	通道接入唯一标识 例如“00000001”
4	请求时间	timeStamp	19	字符串	发起请求的时间：YYYY—MM—DD hh:mm:ss,格式见附录 A 中的表 A.1。 例如“2020-11-10　09:38:01”
5	参数编码	charSet	<=10	字符串	例如“UTF-8”
6	签名方式	signType	<=10	字符串	例如“MD5”
7	签名	sign	32	字符串	签名算法见 7.1.5

表 6　应答公共参数

序号	字段名	参数名	长度	类型	说明
1	应答时间	timeStamp	19	字符串	应答时间：YYYY—MM—DD hh:mm:ss,格式见附录 A 中的表 A.1。 例如“2020-11-10　09:38:01”
2	签名	sign	32	字符串	签名算法见 7.1.5

7.2.2　收单机构注册接口

接口名称：TerminalRegist。

收单机构应向省级清算管理机构请求注册。每个受理终端上线前收单机构应先将终端编号（PSAM 卡号）发到省级清算管理机构登记，上传的交易数据才能被平台受理。注册接口请求参数见表7，返回参数见表8。

表 7　请求参数

序号	字段名	参数名	长度	类型	说明
1	收单机构标识	iManagerId	6	字符串	6 位收单机构标识 例如“010001”
2	终端编号	itermNo	8	字符串	例如“99990001”

表 8　返回参数

序号	字段名	参数名	长度	类型	说明
1	返回码	resultCode	<=8	字符串	0：成功 其他：错误
2	错误消息	errMsg	<=128	字符串	例如“系统错误!”

7.2.3　账单上送

接口名称：BillUpload。

收单机构应向城市发码机构和省级清算管理机构进行账单上送。收单机构将本地交易记录（账单）上传给本地发码机构，发码机构根据上传的账单对用户进行扣费。收单机构将所有交易记录（账单）上传给省级清算管理机构，省级清算管理机构应将跨区交易记录（账单）上传给本地发码机构相应地市发码机构，相应地市发码机构根据上传的账单对用户进行扣费。账单上送请求参数见表9，单条交易记录格式见表10，返回参数见表11。

终端上传二维码交易数据到服务端，采取准实时上传方式，即终端存在未上传交易时，应立即上传交易数据。终端应根据错误的计数延迟上传，每出现一次错误，延迟时间增加30秒，最大延迟时间为300秒。当出现一次响应成功时，复位延迟时间复位。

表 9　请求参数

序号	字段名	参数名	长度	类型	说明
1	交易记录	jList	根据实际字符串长度填写	JSON 字符串	JSON 格式：{{…},{…}….}

表 10　单条交易记录格式

序号	字段名	参数名	长度	类型	说明
1	收单机构标识	acquirerId	6	字符串	6 位收单机构标识 例如“010001”
2	交易标识	tranId	32	字符串	收单机构标识和收单机构交易流水号流水组成，收单机构每上送一笔交易，必须赋予数字交易流水号作为唯一标识，交易重复发送时的交易 ID 须相同，例如 “01000100000000000000000000000001”
3	支付账户号	payAcct	32	字符串	二维码中原数据送回，见 6.2 表 2
4	用户账户号	userId	20	字符串	城市发码机构的用户 id 二维码中原数据送回，见 6.2 表 2
5	城市发码机构代码	cardPlt	8	字符串	见 6.2 表 2
6	发码平台代码	qrPlt	8	字符串	填发码平台代码（当付款方式用），见 6.2 表 2
7	交易金额	totalFee	<=10	整数	单位为分，10 进制
8	应收金额	payFee	<=10	整数	单位分，10 进制

表10　单条交易记录格式（续）

序号	字段名	参数名	长度	类型	说明
9	本次交易时间	tranTime	8	十六进制字符串	使用UTC（0　时区）时间1970年1月1日00：00：00到当前的秒数，高字节在前
10	本次交易终端编号	termNo	8	字符串	交易时终端编号—应取PSAM卡8位终端编号
11	线路编号	lineNo	8	字符串	填入线路编号
12	二维码生成时间	qrTime	8	十六进制字符串	使用UTC（0　时区）时间1970年1月1日00：00：00到当前的秒数，高字节在前
13	经度	lng	8	十六进制字符串	扫码时的终端经度，4字节，共32位，高位在前 第1位：0表示东经，1表示西经 第1-31位表示经度值，以1E-9度为单位
14	纬度	lat	8	十六进制字符串	扫码时的终端纬度，4字节，共32位，高位在前，以1E-9度为单位
15	二维码业务数据	qrBiz	64	字符串	城市发码机构自定义数据内容
16	交易类型	tranType	2	字符串	第1位: 0：普通卡 1：乘车券 第2位： 0：公交消费 1：地铁入闸 2：地铁出闸消费 3：地铁核准交易
17	终端流水号	termSeq	10	字符串	前补“0”
18	站点编号	station	4	字符串	站点名称
19	系统授权过期时间	sysauthTime	8	十六进制字符串	对应二维码中系统授权过期时间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到当前的秒数，高字节在前
20	码类型	qrType	1	字符串	1：正常码 2：应急码
21	外地市二维码数据	allCode	728	十六进制字符串	省外发码机构的二维码在省内受理的，该项必填

表11　返回参数

序号	字段名	参数名	长度	类型	说明
1	返回码	resultCode	<=4	字符串	0：成功 其他：错误
2	错误消息	errMsg	<=500	字符串	例如“系统错误!”

7.2.4 城市发码机构白名单下载接口

接口名称：AcceptCitysInfo。

收单机构应向省级清算管理机构请求城市白名单列表。受理终端通过收单机构下载最新的白名单列表信息。获取白名单请求参数见表12，返回参数见表13。

表 12 请求参数

序号	字段名	参数名	长度	类型	说明
1	收单机构标识	imanagerId	6	字符串	6 位收单机构标识

表 13 返回参数

序号	字段名	参数名	长度	类型	说明
1	城市发码机构白名单列表	whiteList	<1000	字符串	城市发码机构代码列表，逗号分隔
2	返回码	resultCode	<=4	字符串	0：成功 其他：错误
3	错误消息	errMsg	<=500	字符串	例如“系统错误!”

7.2.5 时钟同步接口

接口名称：TimeSynchronize。

收单机构和发码机构应向省级清算管理机构请求时钟同步，受理终端和客户端软件应分别向收单机构和发码机构申请时间同步，服务器返回系统标准时间。时钟同步请求参数见表14，返回参数见表15。

表 14 请求参数

序号	字段名	参数名	长度	类型	说明
1	收单机构标识	imanagerId	6	字符串	6 位收单机构标识
2	终端编号	itermNo	8	字符串	8 位 Psam 卡号

表 15 返回参数

序号	字段名	参数名	长度	类型	说明
1	服务器时间	oserverTime	8	十六进制字符串	使用 UTC（0 时区）时间 1970 年 1 月 1 日 00：00：00 到当前的秒数，高字节在前
2	返回码	resultCode	<=4	字符串	0：成功 其他：错误
3	错误消息	errMsg	<=500	字符串	例如“系统错误!”

8 受理终端要求

受理终端应符合JT/T 978.3和JT/T 1179—2018第10章的要求。

9 客户端软件要求

客户端软件要求应符合JT/T 1179—2018第11章的要求。

10 安全规范

安全规范应符合JT/T 1179—2018第9章的要求。

附 录 A
（规范性）
符号定义表

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
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
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	字母和数字字符，左靠，右边多余位填空格
cn	压缩数字码，即 BCD 码，后跟数字表示 BCD 码的个数
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
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
YYYY	年份，0000～9999
hh	时，00～23
mm	分，00～59
ss	秒，00～59