淄博齐达通交通二维码码结构说明

修订记录

日期	修订 版本	修改 章节	修改描述	作者
20200608	V1.0	新建		李享

目录

1　前言

淄博齐达通交通一卡通二维码数据采用二进制编码方式，编码格式符合 GB/T 18284 的要求。实现完全符合《交通一卡通二维码支付技术规范》（JT/T 1179-2018）要求。

2　二维码数据结构

2.1　数据结构

2.1.1　数据组成

交通一卡通二维码数据主要由17个字段组成，包括：二维码版本、二维码数据长度、发卡机构公钥证书、支付账户号、用户账户号、发卡机构代码、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、发卡机构自定义域长度、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。二维码数据结构见图8。

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	用户账户号	发卡机构代码	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	发卡机构自定义域长度	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	1	32	65	4	65

图1　交通一卡通二维码结构

2.1.2　要求和说明

二维码数据结构各部分的要求及说明见表2。二维码数据结构组成中出现的格式符号要求见附录A。

表1　交通一卡通二维码数据结构组成部分

序号	字段名称	字段长度	字段格式	是否必填	字段说明
1	二维码版本	1	B	M	版本范围0x80～0xFF。
2	二维码数据长度	2	B	M	本表序号第3～17字段的总长度。
3	发卡机构公钥证书	117	B	M	发卡机构公钥证书内容见表18。

4	支付账户号	16	ans	M	由支付账户系统自定义。
5	用户账户号	10	B	M	由发卡机构账户管理平台定义。
6	发卡机构代码	4	B	M	由清分结算机构统一分配。
7	发码平台编号	4	B	M	由清分结算机构统一分配。
8	用户账户类型	1	B	M	用户账户的类型。见JT/T 978.2-2015中表A.1中发卡机构特殊数据元第20字节卡种类型。
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	支付账户用户公钥	33	B	M	经过压缩的支付账户系统中用户公钥数据，压缩方法见GB/T 32918。
11	支付账户系统授权过期时间	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。
12	二维码有效时间	2	B	M	以秒为单位，此域在填写时无需带单位。
13	发卡机构自定义域长度	1	B	M	发卡机构自定义域数据长度，最大32。
14	发卡机构自定义域	N..32	B	C	发卡机构自定义，由发卡机构自定义域。 1、二维码类型（字段长度1，01：普通在线码，02：普通脱机码）； 2、二维码序列号（字段长度12）； 3、二维码脱机码的最大有效期（字段长度4）
15	发卡机构授权签名	65	B	M	发卡机构私钥签名,签名数据包括：本表中序号为3～14字段。
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。
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。

2.2 数据签名

使用 SM2 算法的数据签名见表 3。

表2 数据签名

字段名称	字段长度	字段格式	是否必填	字段说明
签名的数据格式	1	B	M	十六进制，值为‘15’。

数字签名	64	B	M	二维码中数据计算的SM2签名r||s。

2.3 编码格式

交通一卡通二维码数据采用二进制编码方式，编码格式应符合GB/T 18284的要求。