ICS 点击此处添加 ICS 号
点击此处添加中国标准文献分类号

DB44

广　东　省　地　方　标　准

DB 44/ XXXXX—XXXX

广东省城市公共交通二维码应用技术规范

Technical Code for application of Qr Code in urban public transport of Guangdong Province

点击此处添加与国际标准一致性程度的标识

（征求意见稿）

（本稿完成日期：2020-8-27）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

广东省市场监督管理局　　发布

目　　次

前　言

本文件按照 GB/T1.1-2020 给出的规定起草。

本标准由广东省交通运输厅提出。

本标准由广东省交通运输（公路水路）标准化技术委员会归口。

本标准起草单位：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。

本标准主要起草人：谢振东、易智君、刘兵、方秋水、温晓丽、徐锋、何建兵、曾江、袁勇、程世勇、郭贵城、吴金成。

广东省城市公共交通二维码应用技术规范

1 范围

本标准规定了广东省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、终端以及支付终端要求。

本标准适用于广东省公共交通二维码支付终端程序及账户发行方后台服务系统、二维码终端硬件、应用程序、清算管理方、终端管理方后台服务系统、二维码交易风险控制相关系统的设计、研发与应用。

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/T2312　　信息交换用汉字编码字符集　基本集

GB/T18284-2000　　快速响应矩阵码

GB/T32918　　（所有部分）信息安全技术　SM2　椭圆曲线公钥密码算法

3 术语和定义、缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

二维码　Two-dimensional　code

用某种特定的几何图形按一定规律在平面（二维方向上）分布的黑白相间的图形记录数据符号信息的。通过图象输入设备或光电扫描设备自动识读以实现信息自动处理。

3.1.2

受理终端　Terminal

一种安装在公共汽电车、城市轨道交通、轮渡等场景的多功能终端，可实现支付收款功能。

3.1.3

支付终端　Mobile　client

可以在移动终端运行的软件,客户端(Client)或称为用户端,是指与服务器相对应,为客户提供本地服务的程序。

3.1.4

终端管理方　Terminal　administrators

各支付终端管理者（或所有者）所开发的终端后台系统，负责兼容对接各种不同厂家终端，处理交易数据，并按统一格式存储在后台数据库中。

3.1.5

清算管理方 Liquidating administrators

连接终端管理方和账户发行方的系统，负责交易资金的清分结算功能，为各类型资金渠道（账户方）和各终端管理方提供统一的平台对接服务。

3.1.6

账户发行方 Account issuer

用户在交易过程中所使用的资金账户，为用户交易提供资金渠道和管理服务。

3.1.7

密钥 Secret key

在明文转换为密文或将密文转换为明文的算法中输入的参数，分为对称密钥与非对称密钥。

3.1.8

SM2 算法 SM2 algorithm

SM2 是国家密码管理局于 2010 年 12 月 17 日发布的椭圆曲线公钥密码算法。

SM2 算法和 RSA 算法都是公钥密码算法 SM2 算法是一种更先进安全的算法，在我们国家商用密码体系中被用来替换 RSA 算法。

3.1.9

时间戳 Time stamp

一个能表示一份数据在某个特定时间之前已经存在的、完整的、可验证的数据,通常是一个字符序列，唯一地标识某一刻的时间。使用数字签名技术产生的数据，签名的对象包括了原始文件信息、签名参数、签名时间等信息。

3.1.10

安全模块 Secure access module

支持密钥安全存储、运算与验证的黑盒模块。

3.1.11

数字签名 Digital signature

又称公钥数字签名、电子签章，是一种类似写在纸上的普通的物理签名，使用了公钥加密领域的技术实现，用于鉴别数字信息的方法。一套数字签名通常定义两种互补的运算，一个用于签名，另一个用于验证。

3.1.12

密钥分散 Key diversification

一种密钥产生的算法，通过该算法输入主密钥和分散因子可产生一个子密钥，而已知子密钥和分散因子无法推导出主密钥。

3.1.13

离线/脱机交易 Offline trade

交易验证及记帐过程不需要获得后台服务器的验证和许可，即可在终端和支付媒介之间完成交易。离线交易的交易记录通过异步的方式上送到后台服务器。

3.2 符号和缩略语

下列符号和缩略语适用于本文件。

UID:用户账户标识（User Account Identifier）

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

MAC:消息认证码（Message Authentication Code）

QR CODE:快速响应矩阵码（Quick Response Code)

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

4 系统架构

二维码系统由终端管理方、清算管理方、账户发行方、终端及支付终端组成。如二维码系统架构见图 1。

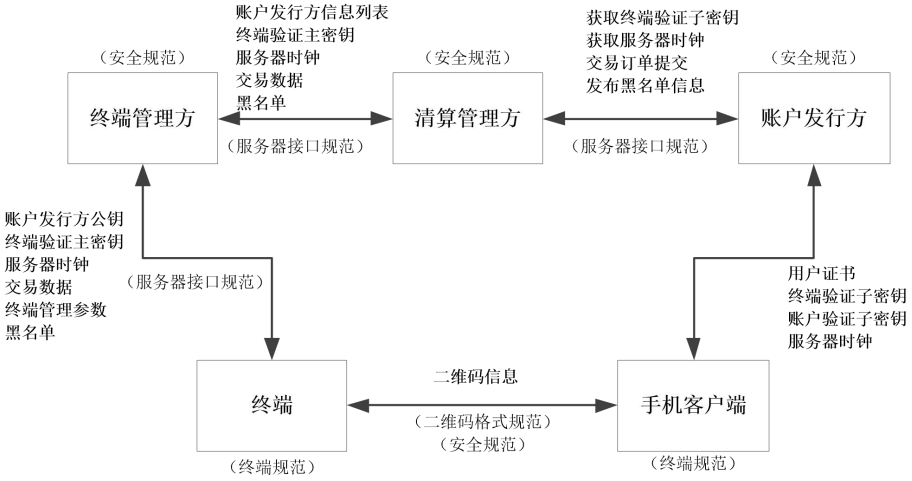

图 1 系统架构示意图

终端管理方和清算管理方之间通过服务器接口交换数据，接口包括获取账户发行方信息、终端验证主密钥、服务器时钟、黑名单，上传交易数据等。

清算管理方和账户发行方之间通过服务器接口交换数据，接口包括获取终端验证子密钥、服务器时钟和发布黑名单，上传交易数据等。

终端和终端管理方之间通过服务器接口交换数据,接口包括获取账户发行方信息、终端验证主密钥、服务器时钟、黑名单、终端管理参数以及上送交易数据和终端状态信息。

支付终端向账户发行方获得产生二维码所需的数据，包括用户证书、终端验证子密钥、账户验证子密钥以及服务器时钟。其中终端验证子密钥和服务器时钟需由账户发行方服务器转发，向清算管理方服务器请求。

支付终端的功能以及二维码的产生方法应符合本规范第 5 章和第 6 章的要求。

受理终端通过接口向终端管理方服务器上传交易数据到清算管理方，并由清算管理方服务器生成订单发送给账户发行方，由账户发行方完成交易结算。

受理终端的功能以及二维码的验证规则应符合本规范第 5 章以及第 7 章部分描述。

5 二维码数据格式

5.1 编码格式

应符合 GB/T18284-2000 的要求。

5.2 数据构成

二维码应由二维码数据头和数据体组成。

5.2.1 数据头

表 1 数据头

内容	长度（字节）	类型	说明
二维码版本号	1	BIN	0x88（部标预留） 二维码数据格式版本
二维码类型	2	BIN	0x88 版本，本字段无意义建议值 0x00
发码方式	1	BIN	0x88 版本，本字段无意义建议值 0x00
发卡机构证书编号	4	BIN	0x88 版本，本字段无意义建议值 0x00

5.2.2 数据体

表 2 数据体

内容	长度（字节）	类型	说明
证书数据	96	BIN	见[证书数据（表 3）]
支付类型	3	BIN	由账户发行方自定义
二维码生成时间	4	BIN	Unix 时间，高字节在前
终端验证 MAC	4	BIN	见[6.1.3.4]
账户验证 MAC	4	BIN	见[6.1.3.4]

5.3 证书数据

表 3 证书数据

内容	长度（字节）	类型	说明

证书版本	1	BIN	证书应用版本 对应终端规则版本， 当前版本为 0x01
算法标识	1	BIN	低 4 位为证书签名算法 1：256 位　SM2 2：1024 位 RSA 3：SM4 国密算法 其他：保留 高 4 位为 MAC 计算算法 0：3DES　MAC 其他：保留

表 3　（续）

内容	长度（字节）	类型	说明
密钥版本	1	BIN	0x01 表示主版本公钥验签 0x02 表示副版本公钥验签 其他：无效
账户发行方标识	3	BIN	唯一标识账户发行方，参见附录 B 描述
用户标识	8	BIN	标识用户账户的编号，单一账户发行方，用户标识唯一
证书签发时间	4	BIN	UNIX 时间值，高字节在前
证书失效时间	4	BIN	UNIX 时间值，高字节在前
二维码失效时间	2	BIN	二维码展示的有效时间，单位秒，高字节在前 失效时间为 0，表示强制联机
应用范围	2	BIN	共 16 位复选开关量 0：不许可 1：许可 第 1 位：　公共汽电车 第 2 位：　城市轨道交通 第 3 位：轮渡 第 4 位：出租汽车 其它：保留
单笔限额	4	BIN	单位分，高字节在前
扩展数据长度	2	BIN	高位在前
扩展数据			见[扩展数据]
签名数据	64/128	BIN	算法标识为 01 时，为长度 64 字节的 SM2 私钥签名数据 算法标识为 02 时，为长度 128 字节

			的 RSA 私钥签名数据

5.4 扩展数据

扩展数据为 TLV 格式数据集合，各数据之间无间隔，TLV 格式定义见表 4。

表 4 TLV 数据格式

内容	长度（字节）	类型	说明
T	1	BIN	定义见[TLV 数据类型]
L	1	BIN	字节数，1-255,L=0 扩展数据解析失败
V	L	BIN	

6 受理终端要求

6.1 功能要求

6.1.1 二维码读码单元

识别精度应在 5mil 以内；
识读码制应可识别但不限于 QR Code(QR 1/2,Micro)
识读角度应可旋转 360°、倾斜+-40°，偏转+-40°

6.1.2 通讯能力要求

具备与后台数据通讯能力，应支持 TCP 协议，通讯速率应>=115200bps。

6.1.3 安全模块单元（可选）

终端 MAC 密钥应存储于安全模块中，如 SAM；
安全模块只具有 MAC 验证功能，不具有密钥导出和加密运算输出功能。
MAC 验证功能输入分散因子和 MAC 值，返回验证成功或验证失败。

6.1.4 实时时钟单元

应采用独立电池供电，误差应 <15PPM，应用程序可修改系统时钟。

6.1.5 存储单元

非易失性存储单元，用于存储交易数据、黑名单及密钥，总容量>=16MB；
非易失性备份存储单元，用于保护未上传交易数据、配置参数等关键数据不被丢失，容量>=256KB。

6.1.6 扫码响应速度要求

二维码进入终端扫描区后，终端扫码响应时间应<=100ms,扫码交易处理总时间应<=600ms；
终端执行网络任务时，不应对扫码响应速度产生影响。

6.2 基本数据元

终端应产生、管理并保存以下数据，如表 5 所示。

表 5　　终端基本数据元

内容	说明
终端编号	终端唯一性标识
终端可支持的证书版本	终端程序对应可支持的证书版本
行业类型代码	表示终端所属的行业 参考[证书数据/应用范围]部分描述
账户发行方信息	终端获取并保存的账户发行方信息，见[附录 B　记录数据格式/账户发行方信息记录]
终端验证主密钥列表	终端通过接口获取并保存的终端验证主密钥列表，见[附录 B 记录数据格式/终端验证主密钥记录]
时钟允许误差	判断二维码生成时间是否有效的误差允许值，单位为妙，默认 5s
未上传交易	终端保存的未上传的交易数据，容量应>=1000 笔，数据格式见[附录 B　记录数据格式/终端上送交易记录]
未上传交易笔数	终端保存的未上传的交易数据的笔数
未上传交易最大笔数	终端可允许的未上传交易最大笔数
已上传交易	终端应保存>=3 日的已上传交易，数据格式见[附录 B　记录数据格式/终端上送交易记录]
紧急黑名单	终端保存通过服务接口获取的黑名单，黑名单的数量>=1000，数据格式见[附录 B　记录数据格式/黑名单记录]
清算管理方服务器信息	清算管理方主服务器和备用服务器地址信息
连续交易超时时间	终端判断是否为连续交易的时间间隔，单位为秒，默认 10s
单一用户间隔时间	单一用户在同一终端两次交易的间隔时间，单位为秒，默认为 60s
立即上传交易笔数	未上传交易笔数达到该值后立即启动上传，默认为 4
终端允许的最大证书有效时间	单位为分钟，默认为 7200 分钟
终端获取黑名单间隔周期	单位为秒，默认为 600s
终端联机更新周期	终端在运行状态下，定期获取账户方发行信息、获取清算管理方时间戳密钥，获取服务器时间的间隔周期，单位为分钟，默认 720 分钟
最大脱机工作周期	终端不能联机的最长工作时间，单位为分钟，默认为 4320 分钟
清算管理方时间戳装载模式	SAM 模式或网络下载模式
终端时间	终端通过实时时钟单元获取的时间值，精确到秒
扫码等待时间	从上一用户扫码识别成功之后的时间，单位为秒

6.3　功能与流程的要求

6.3.1　参数设置

可设置的终端参数包括：终端编号、行业类型代码、清算管理方服务器信息、连续交易超时时间、单一用户间隔时间、立即上传交易笔数、终端允许的最大证书有效时间、终端获取黑名单间隔时间、终端联机更新周期。

6.3.2 获取账户发行方信息列表

终端在启动或运行时间达到“终端联机更新周期”时，终端应向服务器获取最新的账户发行方信息列表；

账户发行方信息应符合[附录 B]的格式。

6.3.3 公钥版本切换

终端检测到证书里的密钥版本为 0x02 时，应切换使用该账户发行方副版本证书验证公钥，直到重新获取新的账户发行方信息成功后，切换为主版本证书验证密钥。

6.3.4 获取服务器时钟

终端启动或运行时间达到“终端联机更新周期”时，终端应向服务器发送获取服务器时钟报文，获取服务器时钟成功后，更新本地时钟。

6.3.5 获取终端验证主密钥列表

若终端验证主密钥装载模式为网络下载模式时，终端在启动或运行时间超过“终端联机更新周期”时，终端应向服务器获取当前日期 5 日内终端验证主密钥列表。

终端验证主密钥格式见[附录 B]。

6.3.6 二维码验证

6.3.6.1 证书标识码检查

判断标识码是否正确，不正确则验证失败；

标识码格式及值见［5.2］。

6.3.6.2 证书版本检查

证书版本与终端可支持的版本是否符合，不符合则验证失败。

6.3.6.3 账户发行方标识检查

判断账户发行方信息列表里是否存在证书里 UIID 对应的账户发行方，不存在则验证失败。

6.3.6.4 黑名单检查

以黑名单序号倒序的方式，以 UIID 和 UID 为条件检索终端本地黑名单列表。

若未找到对应的黑名单则为正常账户；

若找到黑名单且黑名单未过期，则为黑名单；

若找到黑名单且黑名单已过期，则为正常账户。

6.3.6.5 证书有效期检查

终端本地时间小于证书起始时间－时钟误差允许时间，验证失败；

终端本地时间大于证书失效时间＋时钟误差允许时间，验证失败。

6.3.6.6 行业类型检查

终端判断终端所属行业类型对应的证书里的应用范围是否具有支付权限，无则验证失败。

6.3.6.7 证书验签

终端用账户发行方公钥验证证书签名，验签失败则验证失败。

6.3.6.8 二维码生成时间检查

［二维码生成时间］＜［证书起始时间］，验证失败；
［二维码生成时间］＞［证书失效时间］，验证失败；
［终端时间］－［二维码生成时间］＞［二维码失效时间］＋［时钟允许误差］，验证失败；
［终端时间］＋［时钟允许误差］＜［二维码生成时间］，验证失败。

6.3.6.9MAC 验证

1、主密钥产生子密钥（见［安全规范/密钥/终端验证主密钥/子密钥产生过程］）。
2、子密钥计算终端验证码 MAC（见［安全规范/密钥/终端验证子密钥/终端验证 MAC 计算规则］）。
3、比较计算的 MAC 和二维码里的 MAC 是否一致，不一致则验证失败。

6.3.6.10 交易金额检查

终端的交易金额是否大于证书里的单笔限额，大于则验证失败。

6.3.7 交易记录

终端验证二维码为验证成功后，终端提示交易成功；
终端将交易数据存入本地存储器，存储的数据内容见[附录 B]。

6.3.8 交易上传

若［未上传交易笔数］＞［立即上传交易笔数］，执行交易上传；
若［扫码等待时间］＞［连续交易超时时间］，执行交易上传；
若［未上传交易笔数］大于［未上传交易最大笔数］，暂停扫码，强制执行交易上传。

6.3.9 交易结算

清算管理方服务器接收到终端管理方上传的交易记录后,应立即生成交易订单发送给账户发行方服务器进行交易结算；
结算交易的记录格式见[附录 B]；
账户发行方应对每笔交易响应对应的交易验证结果，其定义见[附录 A]。

6.3.10 黑名单下载

终端启动或运行时间达到［终端获取黑名单间隔周期］时，终端应向服务器获取最新的黑名单信息列表，获取黑名单成功后，若存在更新则更新本地［黑名单列表］；
黑名单信息应符合［附录 B］的格式。

6.3.11 网络故障处理要求

终端发送［获取账户发行方信息］、［获取终端验证主密钥］、［获取服务器时间］、［获取黑名单］报文出现网络故障时，若终端本地存在有效的账户发行方信息、终端验证主密钥，终端应进入工作状态，而不以阻塞方式继续等待服务响应成功；

当网络故障时间超过［最大脱机工作周期］时，终端则必须阻塞方式等待服务响应成功。

7 支付终端要求

7.1 基本数据元

支付终端应产生、管理并保存以下数据,如表 6 所示。

表 6　　支付终端基本数据元

内容	说明
用户证书	从服务器获取的用户证书数据
终端验证子密钥	见[安全规范/密钥/终端验证子密钥]
账户验证子密钥	见[安全规范/密钥/账户验证子密钥]
二维码展示有效时间	证书里获取的二维码展示有效时间
二维码展示时间	支付终端显示二维码的计时时间，单位为秒
移动设备时钟	当前的移动设备本地时间值
时钟误差	支付终端通过获取服务器时间接口，获得的服务器时间和移动设备时钟的差值，有符号整数，单位为秒
最后同步时钟时间	上一次成功执行同步时钟的移动设备时钟
同步时钟间隔周期	单位为秒
账户发行方服务器信息	账户发行方主服务器和备用服务器地址信息

7.2 功能及流程

7.2.1 时钟同步

若［移动设备时钟］－［最后同步时钟时间］＞［同步时钟间隔周期］，移动设备向清算管理方服务器获取服务器时钟；

获取成功后，计算［时钟误差］＝［移动设备时钟］－［服务器时间值］，本地存储［时钟误差］。

7.2.2 获取二维码生成数据

若用户证书不存在、证书有效期已过期或用户手动刷新时，支付终端通过账户发行方自定义的接口获取生成二维码所需的数据，包括证书数据，终端验证子密钥，账户验证子密钥，其方式如图 3 所示：

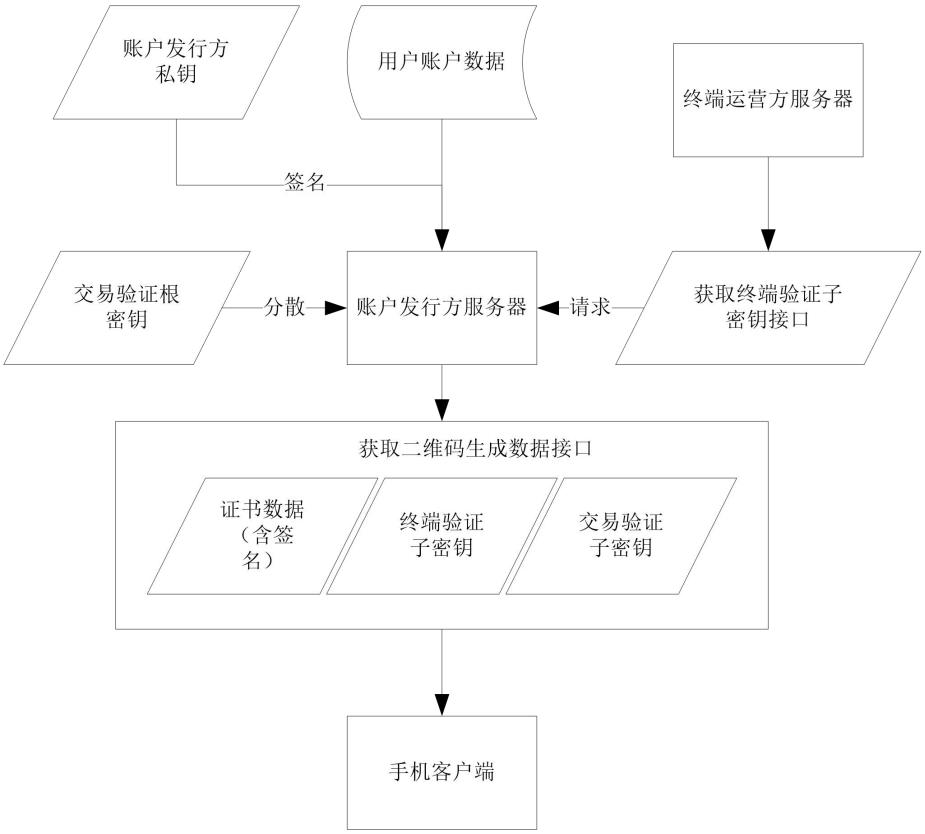

图 2　　支付终端获得二维码生成数据示意图

账户发行方服务器通过接口，向清算管理方服务器请求获取终端验证子密钥；

证书生成规则见［5.3］章节描述；

账户验证子密钥生成规则见［8.1］章节描述；

获取二维码生成数据成功后，移动设备本地存储证书数据、终端验证子密钥，账户验证子密钥于安全区域。

7.2.3　二维码生成

判断移动设备时钟是否大于证书过期时间，大于则执行“获取二维码生成数据”；

用户选择支付方式（账户发行方自定义）；

获取移动设备机器时间加减去偏差值进行校正，获得校准后的时间；

用账户验证子密钥计算账户验证 MAC；

用终端验证子密钥计算终端验证 MAC；

按照本规范第 5 章节要求，生成二维码数据后，生成二维码图片并显示。

7.2.4　二维码周期更新

当［二维码展示时间］＞［二维码展示有效时间］时，支付终端重新生成二维码。

7.2.5　支付信息安全

二维码支付过程中个人信息不应泄露，二维码支付过程中的关键敏感信息加强保护。

8 安全规范

8.1 密钥

8.1.1 证书签名密钥

8.1.1.1 用途

私钥产生对证书明文数据的电子签名；
公钥对证书签名进行验证。

8.1.1.2 密钥类型

应使用 256 位 SM2 非对称密钥对，SM2 算法应符合国家密码局颁布的《SM2 椭圆曲线公钥密码算法》和《SM2 密码算法使用规范》。

8.1.1.3 密钥管理

密钥对由账户发行方生成与管理；
账户发行方应生成两对密钥对，分别为主版本密钥对及副版本密钥对；
私密钥保存在安全设备中，公钥经清算管理方，通过终端管理方下载到终端。

8.1.1.4 签名计算过程

计算证书明文数据的 MD5 值，长度为 32 字节；
使用 SM2 私密钥对 32 字节进行签名，获得 64 字节签名数据。

8.1.2 终端验证主密钥

8.1.2.1 用途

用于产生终端验证子密钥。

8.1.2.2 密钥类型

3DES 密钥应采用 16 字节。

8.1.2.3 密钥管理

由清算管理方生成并管理，密钥存储于安全设备中；
若采用随机数生成方式，清算管理方每日产生一个对应日期的密钥，并通过接口协议下发到终端；
若采用固定密钥方式，密钥存储于安装在终端的安全认证模块（SAM）中。

8.1.2.4 子密钥产生过程

主密钥对“UIID（3 字节）+用户 ID 后 5 字节”做分散，获得一级分散密钥；
一级分散密钥对“证书启用日期（4 字节）+证书失效日期（4 字节）”分散获得子密钥。

8.1.3 终端验证子密钥

8.1.3.1 用途

用于计算终端验证 MAC。

8.1.3.2 密钥类型

3DES 密钥应采用 16 字节。

8.1.3.3 密钥管理

由清算管理方管理的终端验证主密钥分散产生；
账户发行方通过报文接口（附录 A）获取。

6.1.3.4 终端验证 MAC 计算规则

子密钥对“（证书签发日期（4 字节）+二维码生成时间（4 字节）+支付类型（3 字节）+账户验证 MAC（4 字节）”计算 MAC；
MAC 计算算法见[8.2]。

8.1.4 账户验证主密钥

8.1.4.1 用途

用于产生账户验证子密钥。

8.1.4.2 密钥类型

3DES 密钥应采用 16 字节。

6.1.4.3 密钥管理

由账户发行方生成并管理，密钥存储于安全设备中。

8.1.4.4 子密钥产生过程

1、主密钥对“UIID（3 字节）+用户 ID 后 5 字节”做分散，获得一级分散密钥；
2、一级分散密钥对“证书启用日期（4 字节）+证书失效日期（4 字节）”做分散获得子密钥。

8.1.5 账户验证子密钥

8.1.5.1 用途

用于计算账户验证 MAC。

8.1.5.2 密钥类型

3DES 密钥应采用 16 字节。

8.1.5.3 密钥管理

由账户发行方管理的账户验证主密钥分散产生；
支付终端通过报文接口（账户发行方自定义）获取。

8.1.5.4 账户验证 MAC 计算规则

子密钥对“（证书签发日期（4 字节）+二维码生成时间（4 字节）+支付类型（3 字节）”计算 MAC。
MAC 计算算法见[7.2.2]。

8.2 算法

8.2.1 3DES 密钥分散

分散密钥=原 3DES 密钥对“分散因子（8 字节）+分散因子取反值（8 字节）”的 3DES 加密值（16 字节）。

8.2.2 MAC 计算

应使用 16 字节 3DES 密钥，计算步骤如下：

取 8 个 16 进制数 00,00,00,00,00,00,00,00 为初始值；

将需要计算 MAC 的数据分成 8 字节为单位的数据块，标号为 D1，D2..Dn。最后的数据块 Dn 可能是 1-8 个字节。

如果最后的数据块长度是 8，在其后加上 16 进制数 80,00,00,00,00,00,00,00。如果最后的数据块长度等于 7，在其后加上 16 进制数 80。如果最后的数据块小于 7，则在其后加入 16 进制数 80，再重复加入 16 进制数 00，直到达到 8 字节。

对这些数据使用相应密钥加密，计算过程如图 3 所示。

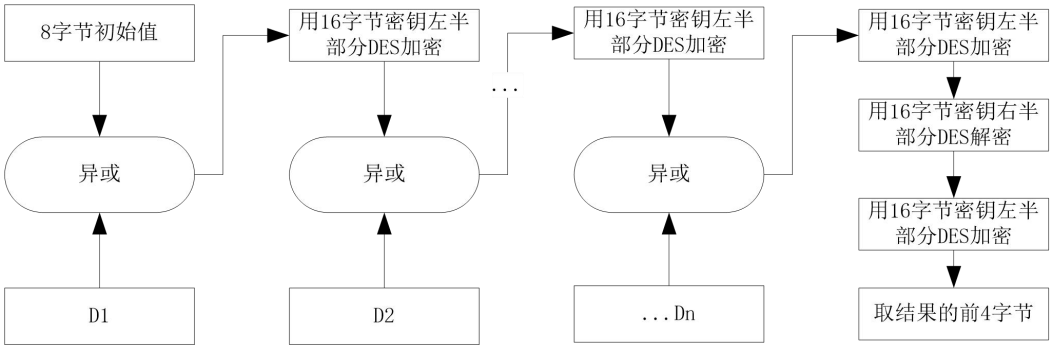

图 3　　MAC 计算过程示意图

8.3 安全设备

可安全存储密钥并进行安全计算的设备或模块，如加密机或 SAM。应通过国家密码管理局的技术鉴定并获得商用密码产品的登记证书。

加密机应具备 SM2 密钥生成及计算能力。

附 录 A
（规范性附录）
数据定义

A.1 账户发行方标识编码

账户发行方标识（UIID）由6位数字组成，其中高1-2位为行业类型，后3-6位为该行业下分配的序号，表列举已登记并分配的账户发行方UIID。新增发行方UIID需对列表进行增补。

表A.1 账户发行方标识表

行业类型	序号	意义
00（城市一卡通）	市以上区域行政编码前 4 位	城市名称
	4401	广州
	4406	广佛通
	其他	保留
01（第三方支付）	0001	财付通
	0002	支付宝
	其他	保留
02（银行）	0001	工商银行
	其他	保留

为确保账户所有方在不同城市的编号唯一以确保互通性，UIID 采取统一注册方式。

A.2 交易验证结果

表A.2 交易验证结果

验证结果	意义
00	收单成功
01	止付卡交易
02	TAC 验证失败
03	交易时间错误
04	交易金额超限
05	交易记录格式错
06	证书片段错误
07	付款方式错

08	站点信息错误
09	账户标识错误
10	交易存在风险
91	订单收款成功
99	系统错误

A.3 TLV数据类型

表A.3 TLV数据类型

T	L	说明
01	4	城市编号
02	2	预设入闸站点或上车站点
03	2	预设出闸站点或下车站点
04	4	预付金额
05	4	预设车辆号
06	1	用户特征 00 普通用户 01 学生 02 老人 60--65 03 残疾人 04 游客 05 VIP 06 老人 65 以上 07 特种卡 08 公安反扒卡
07	8	用户姓名
08	1	性别
09	10	身份证号
0A	4	信用分

附 录 B
（规范性附录）
记录数据格式

B.1 账户发行方信息记录

表B.1 账户发行方信息记录

字段名	偏移	类型	说明
账户发行方标识	0	String(6)	
主版本公钥	6	String(128)	十六进制字符串
副版本公钥	134	String(128)	十六进制字符串
帐户发行方简称	262	String(10)	UTF-8 编码，中文字符或全角字符

B.2 终端验证主密钥记录

表B.2 终端验证主密钥记录

字段名	偏移	类型	说明
起始时间	0	String(8)	UNIX 北京时间戳，16 进制字符串，高字节在前，大写
结束时间	8	String(8)	UNIX 北京时间戳，16 进制字符串，高字节在前，大写
MAC 密钥	16	String(32)	十六进制字符串

B.3 终端上送交易记录

表B.3 终端上送交易记录

字段名	偏移	类型	说明
交易时间	0	String(8)	UNIX 北京时间戳，16 进制字符串，高字节在前，大写
账户发行方 ID	8	String(6)	
账户 ID	14	String(16)	
证书起始时间	30	String(8)	UNIX 北京时间戳，16 进制字符串，高字节在前，大写
证书结束时间	38	String(8)	UNIX 北京时间戳，16 进制字符串，高字节在前，大写
证书片段	46	String(16)	16 进制字符串，证书后 8 字节

二维码生成时间	62	String(8)	UNIX 北京时间戳，16 进制字符串，高字节在前，大写
付款方式	70	String(6)	
交易金额	76	String(8)	单位为分，十六进制字符串
账户验证 MAC	84	String(8)	
交易类型	92	String(2)	00 公交消费 01 地铁入闸 02 地铁出闸消费
终端流水号	94	String(8)	十六进制字符串
终端编号	102	String(8)	
扩展使用	128		用于扩展

B.4 黑名单记录

表B.4 黑名单记录

字段名	偏移	类型	说明
黑名单序号	0	String(8)	
账户发行方标识	8	String(6)	
用户标识	14	String(16)	
止付类型	30	String(2)	00: 正常（白名单） 01：信用异常 02：账户异常 03：用户挂失 其他：保留
过期时间	32	String(8)	UNIX 北京时间戳，16 进制字符串，高字节在前，大写

注意：终端检查黑名单时，如果单一用户存在多个黑名单项时，以序号高的黑名单为准。

B.5 结算交易记录

表B.5 结算交易记录

字段名	偏移	类型	说明
交易 ID	0	String(32)	
城市 ID	32	String(6)	
终端编号	38	String(8)	
交易时间	46	String(8)	
账户发行方 ID	54	String(6)	

账户 ID	60	String(16)	
证书起始时间	76	String(8)	十六进制字符串，高字节在前
证书结束时间	84	String(8)	十六进制字符串，高字节在前
证书片段	92	String(16)	十六进制字符串，证书后 8 字节
二维码生成时间	108	String(8)	十六进制字符串，高字节在前
付款方式	116	String(6)	
交易金额	122	String(8)	单位为分
实扣金额	130	String(8)	单位为分
账户验证 MAC	138	String(8)	
交易类型	146	String(2)	00 公交消费 01 地铁入闸 02 地铁出闸消费 03 地铁核准交易
入闸交易时间	148	String(8)	十六进制字符串，非地铁出闸交易时，填全 0

B.6 结算交易应答记录

表B.6 结算交易应答记录

字段名	偏移	类型
交易 ID	0	String(32)
验证结果	32	String(2)

参 考 文 献

GB/T2312	信息交换用汉字编码字符集　基本集
JR/T　0025.7	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
JT/T978.1-2015	城市公共交通IC卡技术规范　第1部分：总则
JT/T978.2-2015	城市公共交通IC卡技术规范　第2部分：卡片
JT/T978.3	城市公共交通IC　卡技术规范　第3部分：读写终端
JT/T978.4-2015	城市公共交通IC卡技术规范　第4部分：信息接口
JT/T978.6-2015	城市公共交通IC卡技术规范　第6部分：安全