ICS 点击此处添加 ICS 号
点击此处添加中国标准文献分类号

中华人民共和国国家标准

GB/T XXXXX—XXXX
[a]

城市智慧卡二维码应用技术要求

点击此处添加标准英文译名

[b]（征求意见稿）

[c] 20171023

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准由住房和城乡建设部提出。

本标准由全国智能建筑及居住区数字化标准化技术委员会（SAC/TC 426）归口。

本标准起草单位：

本标准主要起草人：

城市智慧卡二维码应用技术要求

1 范围

本标准规定了城市智慧卡二维码在城市综合交通和住区应用的系统要求、系统管理、业务接口文件和清分清算文件等。

本标准适用于城市智慧卡二维码在城市综合交通和住区应用的设计、建设和运营等。

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，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。

GM/T 0003 《SM2椭圆曲线公钥密码算法》

GM/T 0004 《SM3密码杂凑算法》

GM/T 0002 《SM4分组密码算法》

ITU X.509 《Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks》

3 术语和定义

下列术语适用于本文件。

3.1

先充后乘 Prepaid mode

公交二维码支付的一种模式，用户需先在二维码客户端建立虚拟电子卡账户并预付一定资金，乘车时验证用户身份并在交易记录上传后从虚拟电子卡绑定的支付账户中扣除相应的费用。

3.2

先乘后付 Postpaid mode

公交二维码支付的一种模式，给予用户一定授信，乘车时仅验证用户身份，交易记录上传后再支付相应的费用。

3.3

单次交易 Single transaction

受理终端对二维码进行一次验证即可生成一笔交易记录的交易方式。

3.4

复合交易 Composite transaction

受理终端对二维码进行多次验证才能生成一笔交易记录的交易方式。

3.5

互联互通 City union

实现城市智慧卡二维码跨机构支付或身份认证功能的应用。

3.6

互联互通标识 City union code

由二维码互联互通云平台统一管理，参与互联互通机构的统一标识。

3.7

双脱机 Double offline mode

二维码客户端可以脱机生成二维码、受理终端可以脱机验证二维码的机制。

3.8

本地二维码交易 Local QR code transactions

二维码交易地与二维码所属地为同一个城市的交易。

3.9

异地二维码交易 Nonlocal QR code transactions

二维码交易地与二维码所属地为不同城市的交易。

3.10

二维码客户端 QR code application

安装在手机上用于完成二维码支付或认证的应用，二维码申请、展示、记录查询的载体。

3.11

二维码客户端应用后台 QR code application platform

应用后台

二维码客户端的后台应用服务系统，负责二维码客户端信息交互和管理。

3.12

虚拟电子卡号 Virtual electronic card number

由发卡机构分配和管理的用于表征公交二维码的惟一代码。

3.13

支付账户号 Pay account number

由发卡或发码机构分配和管理，与虚拟电子卡号一一绑定，用于公交二维码交易资金结算的账户代码。

3.14

发卡机构 Card issuer

城市级公交支付运营单位，发行城市公交虚拟电子卡，完成本地二维码交易清分结算及异地二维码交易记录上传的机构。

3.15

发码机构 QR code issuer

具备生成二维码的企业，负责用户二维码支付账户号的分配和二维码关联资金的风险管理。

3.16

受理终端 Point of sale

在交易点安装、用于与二维码客户端配合共同完成二维码交易的设备。

3.17

收单机构 Acquirer

二维码支付中受理终端的运营机构。

3.18

二维码互联互通云平台 QR Code Application platform of city union

云平台

用于二维码支付中安全认证管理、异地交易记录转发和异地交易清分结算的系统。

3.19

主扫 Active scanning

二维码支付或认证的一种验证形式，通过受理终端等设备生成并显示二维码，手机二维码客户端主动扫描二维码的验证方式。

3.20

被扫 Passive scanning

二维码支付或认证的一种验证形式，手机二维码客户端生成并显示二维码，被受理终端等设备扫描的验证方式。

3.21

请码 Apply for QR

二维码客户端向发卡/发码机构申请二维码联机数据的过程。

3.22

发码 Release QR Code

请码流程的响应过程，即发卡/发码机构向二维码客户端下发二维码联机数据的过程。

3.23

生码 Generate QR Code

二维码客户端将二维码联机数据和脱机数据组成并展示二维码的过程。

3.24

验码 Verify QR Code

指受理终端验证手机客户端二维码数据的过程。

3.25

纸质票证 Paper ticket

用于二维码展示的载体、介质，可将二维码信息打印在上面。

4 缩略语和符号

下列缩略语和符号适用于本文件。

A 大写字母，左靠，右部多余部分填空格
AES 一种采用区块加密标准的密码算法
ANS 字母、数字和/或特殊符号，左靠，右部多余部分填空格
B 二进制数
BCD 压缩数字码
CA 认证中心(Certificate Authority)
HHMMSS 时、分、秒（Hour，Minute，Second）
ID 身份或账户信息（Identification）
N 数值0~9；右靠，左补零；负号（—）使用“0X2D”，左靠，如—00001表示“—1”
QR 一种可快速读取的二维码编码方式（Quick Response）
RS 一种纠错能力很强的特殊的非二进制码（Reed-Solomon）
S 特殊符号，左靠，右部多余部分填空格
SE 硬件安全模块（Security Element）
SM2 一种椭圆曲线公钥密码算法
SM3 一种密码杂凑算法
SM4 一种对称加密算法
TEE 可信执行环境（Trust Execution Environment）
YYYYMMDD 年、月、日（Year，Month，Day）

5 系统要求

5.1 系统架构

公交支付二维码系统架构如图1所示。

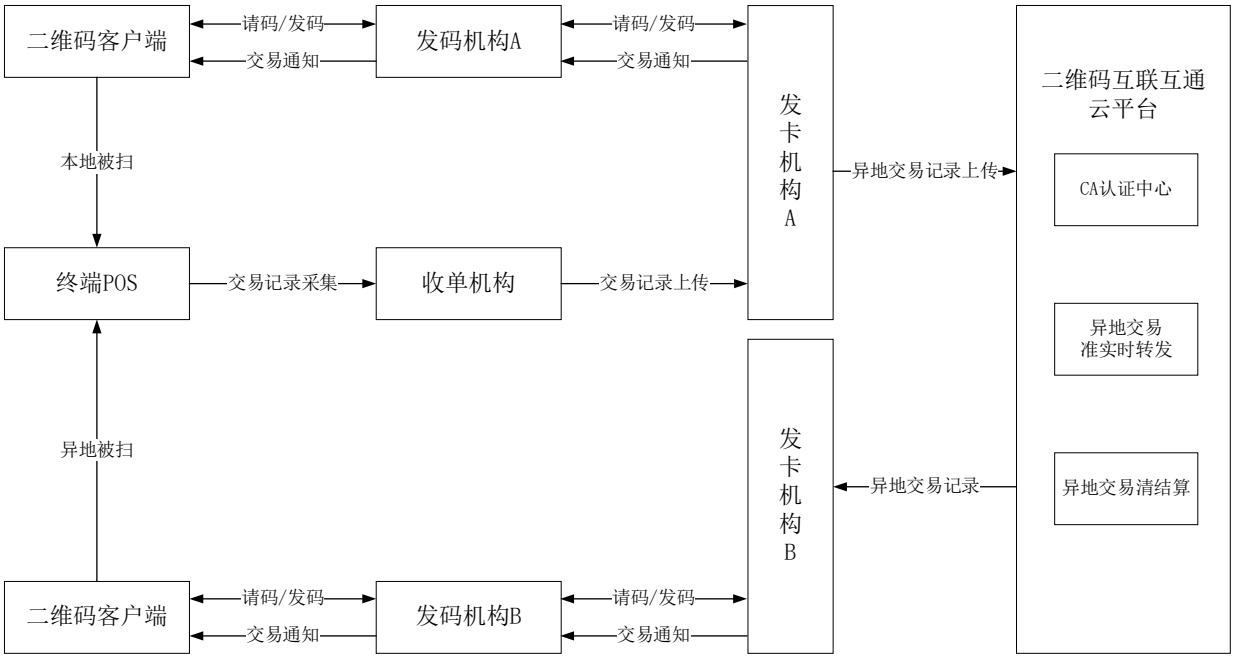

图1 公交支付二维码系统架构

系统中各相关机构应具备以下功能：

a) 发码机构：向云平台申请机构证书的主体，完成请码、发码业务逻辑处理，负责二维码数据的生成和加密处理，提供用户支付账户号；

b) 收单机构：受理终端的运营机构，负责二维码数据验证、预处理和原始交易数据的采集。受理终端中需存放必要的证书作为安全认证使用；

c) 发卡机构应具备下列要求：

1) 二维码虚拟电子卡的生成、分配、注销等生命周期管理的机构；
2) 负责本地二维码交易清分结算；
3) 对接云平台，负责异地二维码交易数据上传。

d) 云平台应具备下列要求：

1) 接收二维码交易地发卡机构上传的异地交易数据，并转发给二维码所属地发卡机构；
2) 对接发卡机构，完成异地二维码交易中发卡机构间的清分、结算；
3) 证书管理，负责为发码机构签发机构公钥证书。

5.2 业务流程

公交二维码支付的业务流程主要包括了开通、请码、发码、生码、验码、交易转发及清分结算等。业务流程如图2所示。

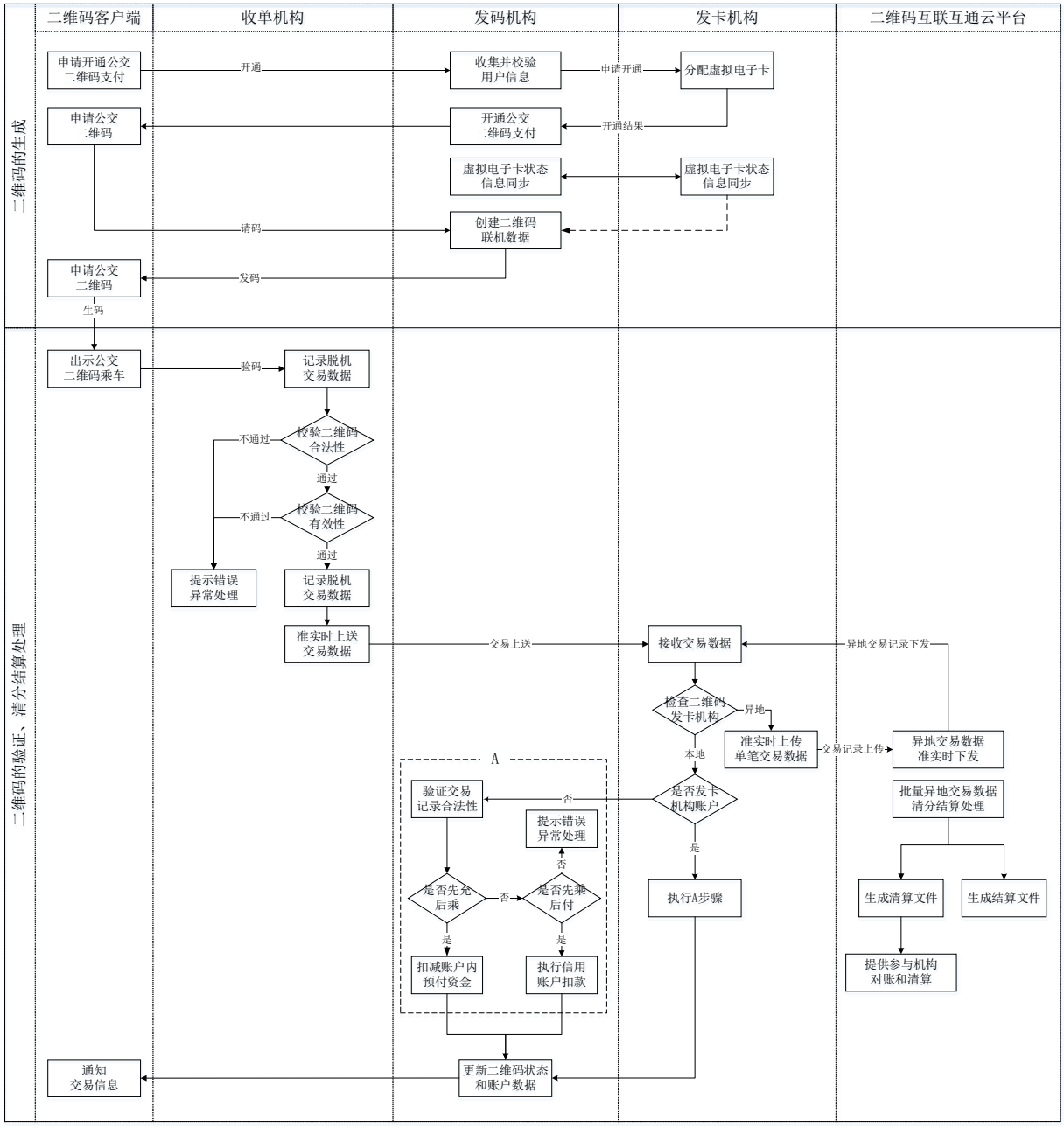

图2　公交支付二维码业务流程图

业务流程说明见表1。

表1　公交支付二维码业务流程说明

序号	步骤	参与方	说明
1.	开通	用户 发码机构 发卡机构	用户与发码机构、发卡机构签署二维码乘车业务协议，选择先充后乘或先乘后付业务，具体业务流程不在本规范规定范围
2.	请码	用户 发码机构	用户通过二维码客户端提交个人实名信息，向发码机构请求二维码联机数据

3.	发码	用户 发码机构 发卡机构	发卡机构为用户分配虚拟电子卡号； 发码机构创建二维码联机数据、发码机构授权信息签名数据
4.	生码	二维码客户端	二维码客户端将发码机构下发的联机数据和自身生成的脱机数据合并，生成并展示二维码
5.	验码	用户 发码机构 受理终端	受理终端对二维码的联机数据和脱机数据进行双重验证，从而保证二维码的合法性和有效性。验证通过后允许用户乘车，受理终端记录该笔交易数据
6.	交易 上送	发码机构 收单机构 发卡机构 云平台	受理终端将交易记录上送发卡机构，发卡机构对交易记录做如下处理： a) 对本地二维码交易数据，完成收单机构的清分、结算处理；完成用户的扣款，并同步信息到发码机构，发码机构通过应用后台下发交易通知到用户；用户扣款存在以下两种模式： 1) 先充后乘：扣减用户预先充值的账户余额； 2) 先乘后付：扣减用户的信用额度。 b) 对于异地二维码交易数据：将交易记录上传至云平台
7.	异地交易 记录转发	云平台 发卡机构	云平台接收二维码交易地发卡机构上传的异地交易数据并转发给二维码所属地发卡机构。
8.	异地交易 清分结算	云平台	云平台采用 T+1 日的方式对交易数据进行跑批：下发清算文件，完成发卡机构间的清分，同时生成结算文件，根据结算文件完成划款结算。
注：在具体业务中，发卡机构与发码机构可以是同一个主体。			

6 二维码管理系统

6.1 双脱机模式

为适应公交快速支付的场景要求，二维码交易采用双脱机的模式：二维码客户端可脱机生成一定数量的乘车二维码供受理终端机脱机扫码，即在脱机状态下完成二维码的生码、验码环节。但在如下情况下，二维码客户端需强制联机并获取授权信息：

a) 用户在首次开通公交二维码支付业务时；
b) 用户重新安装二维码客户端时；
c) 二维码数据中“发码机构授权过期时间”过期时；
d) 用户脱机产生的二维码批次号超出系统限制时。

6.2 实名制

针对公交二维码应用场景的特殊性，用户申请开通二维码支付时需要完成实名验证：

a) 涉及资金垫付：在公交二维码支付业务开通环节，可选择使用先乘后付的信用支付方式。该方式给予用户一定授信，需要对用户的身份进行实名认证，用于登记、维护用户的信用数据及资金风险管控；

b) 涉及卡类型的分配：在公交二维码支付业务请码环节，需要对用户的身份进行实名认证，以便发卡机构确定并分配对应的虚拟电子卡类型（普通卡、老年卡等）；
c) 涉及黑/白名单控制：支付过程采用双脱机模式，对于存在交易及信用异常的用户，其黑/白名单的管理需在二维码客户端完成。因此客户端需要对用户的身份进行实名认证，从而用于支付过程中的支付权限控制。

6.3 密钥管理

6.3.1 一般规定

公交二维码采用三级密钥进行保护，包含CA认证中心级密钥、发卡/发码机构级密钥、发码机构用户级密钥。其中机构级密钥的合法性和有效性需采用CA中心签名保证，发码机构用户密钥由机构级私钥签名保证。涉及公交二维码的证书均采用国密SM2非对称算法（参见GM/T 0003）。各级密钥创建采用硬加密模式，确保密钥的不被篡改和泄露。

为支持离线生成二维码,发码机构用户密钥安全存储于二维码客户端中，此时应保证手机终端密钥存储的安全性。手机终端密钥管理应当满足包括但不限于以下要求：

a) 密钥生成应当满足一机一密，加密密钥的生成因子考虑包含随机因子、设备信息、APP 信息、用户 ID 等；
b) 密钥在二维码客户端内应当采用安全存储，例如采用 SE、TEE、黑匣子等安全策略，确保密钥机密性和完整性；
c) 加密数据的存储和可访问性应该满足设备隔离、应用隔离、用户隔离，即加密后的数据，不能被同一个二维码客户端的其他用户访问，也不能被手机其他客户端访问，同时不能直接拷贝到其他设备的相同文件目录下直接使用；
d) 密钥有效性应当根据安全风控严格控制离线有效时间，过期自动联网刷新；
e) 密钥有效性应当根据安全风控严格控制离线访问次数，次数超限自动联网刷新；
f) 二维码客户端在线时应当定期刷新密钥有效性，至少确保每日联网刷新；
g) 用户更换登录设备时应当需重新身份验证并重新生成密钥，并阻断旧设备访问，作废旧设备上的数据。敏感加密数据需要与设备绑定，如果用户在非绑定设备使用本业务，需要重新验证用户身份，绑定新设备，并作废之前绑定设备上的相关敏感数据。
h) 二维码客户端应当确保相关代码安全，例如采用混淆、加壳、加密等技术防止机密信息被静态分析、逆向调试等攻击；
i) 二维码客户端应当确保密钥数据运行环境安全，例如采用病毒木马检测等技术防止攻击。

6.3.2 密钥机制

发码机构将机构证书和CA根证书下发至受理终端。在机构证书下发中，CA根证书需要对机构证书合法性进行检查，发码机构私钥由发码机构自行保管并保证其安全性。发码机构自行管理用户公私钥对的生成机制，用户私钥由发码机构私钥签名保证其安全性，密钥机制见图3。

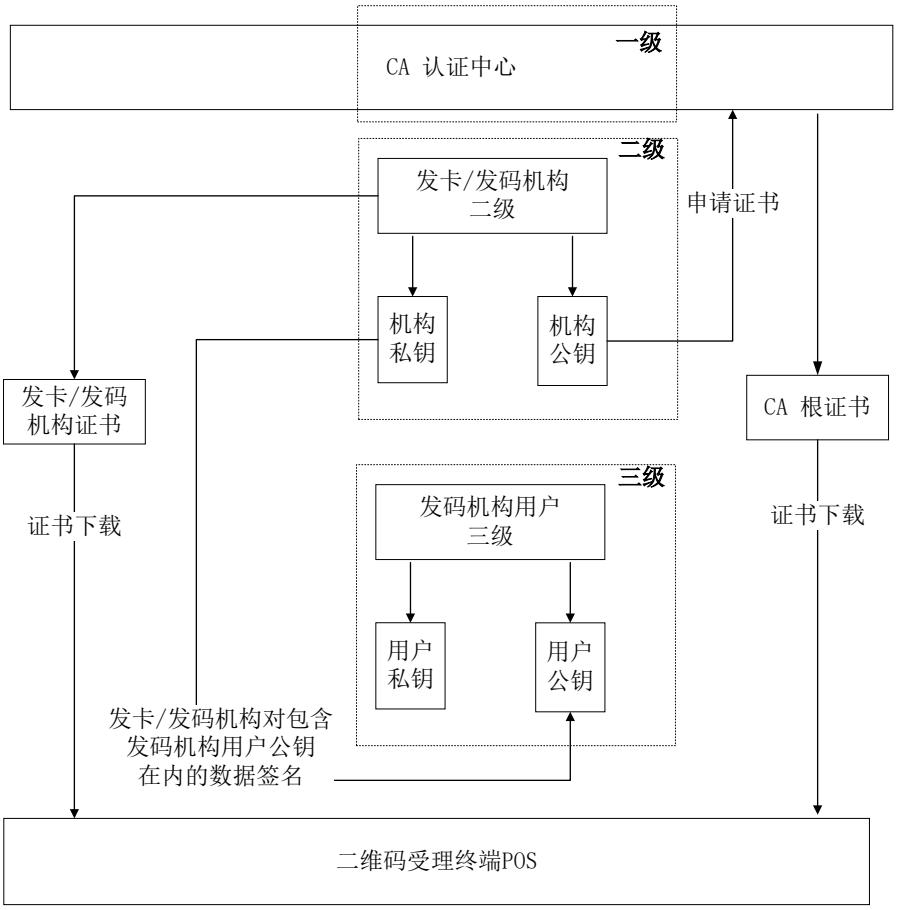

图3　密钥机制

6.3.3　签名验证机制

6.3.3.1　流程

签名验证机制的流程见图4。

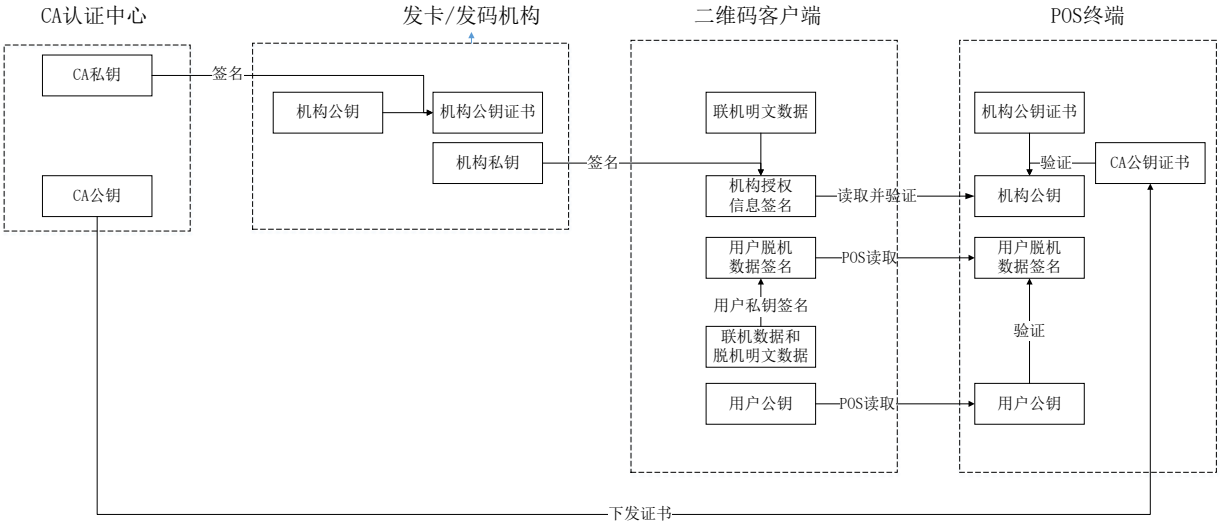

图4　签名验证机制流程

6.3.3.2 签名过程

签名过程应符合下列要求：

a) CA 认证中心：生成 CA 公钥和 CA 私钥，并符合下列要求：
   1) CA 私钥：用于签发机构公钥证书；
   2) CA 公钥：下发 CA 根证书至 POS，用来验证 POS 中机构公钥证书的合法性。
b) 发卡/发码机构：生成机构公钥、机构私钥，管理用户公钥、用户私钥，并符合下列要求：
   1) 机构公钥：提交至 CA 认证中心，获取 CA 认证中心签发的机构公钥证书；
   2) 机构私钥：机构自行保存，用于签名二维码数据组成中的联机数据。
c) 二维码客户端：存放用户公钥、用户私钥、机构授权信息签名、用户脱机数据签名，并符合下列要求：
   1) 用户公钥：作为联机数据的一部分，由机构私钥签名得到机构授权信息签名；
   2) 用户私钥：用于签名二维码的所有数据，生成用户脱机数据签名。

6.3.3.3 验证过程

验证过程应符合下列要求：

a) 机构授权信息签名的验证：受理终端读取二维码数据，获取机构授权信息签名，用设备中存放的机构公钥用验证机构私钥签名过的机构授权信息签名；
b) 用户脱机数据签名的验证：受理终端读取二维码数据，获取用户公钥和用户脱机数据签名，用用户公钥验证用户私钥签名过的用户脱机数据签名。

6.3.4 证书格式

机构证书采用标准的CER格式的X.509证书。机构证书格式见表2。

表2 机构证书格式

序号	字段名	描述
1.	版本	十六进制，值为‘V3’
2.	序列号	云平台分配的机构证书序列号
3.	签名算法	SM3WithSM2 （1.2.156.10197.1.501）
4.	颁发者	CN = CA 颁发机构（简称） O= CA 颁发机构（汉字） C = CN（中国）
5.	有效期	5 年
6.	使用者	CN =发码机构代码+流水编码 O = 使用者单位名称全称（汉字） C = CN（中国）

6.4 二维码的组成

公交二维码由联机数据和脱机数据组成，公交二维码数据结构见表3。二维码客户端在展示城市智慧卡二维码时，应该在二维码中心位置显示具有附录A要求的统一互联互通标志。

表3　公交二维码数据结构

类别	序号	字段名	长度	描述	格式
联机数据	1.	标识	2	城市智慧卡二维码标识	ANS 取值：CJ
	2.	版本号	1	二维码的版本号	B
	3.	互联互通标识	1	00 －可互联互通 其他 －不可互联互通	B
	4.	发码机构代码	8	发码机构号（云平台统一分配）	BCD 机构代码长度为15位： 例：000000000000000，实际转换为 “\x00\x00\x00\x00\x00\x00\x00\x0F”
	5.	发卡机构代码	8	发卡机构号（云平台统一分配）	BCD 机构代码长度为15位： 例：000000000000000，实际转换为 “\x00\x00\x00\x00\x00\x00\x00\x0F”
	6.	证书编号	2	由CA认证中心分配，即发码机构证书“使用者”CN项的流水编码。	BCD
	7.	验码方式	1	1 － 联机方式 2 － 脱机方式	N
	8.	发卡机构保留数据长度	1	发卡机构保留数据的长度	B
	9.	发卡机构保留数据	依赖表3.8	由发卡机构自行定义，可定义行业应用类别、应用场景等，	B 最大不超过20
	10.	二维码有效时长	2	二维码从创建开始到失效间的时间，以秒为单位。	BCD
	11.	卡类型	1	卡类型 00 － 普通卡 01~XX －发卡机构自行定义	BCD
	12.	用户唯一识别号	10	虚拟电子卡号（发卡机构分配）	BCD
	13.	支付账户号长度	1	支付账户号的长度，由发码机构定义。	BCD

	14.	支付账户号	依赖表3.13	用于二维码支付的客户端账户资金账户，与用户唯一识别号一一对应	B 最大不超过20
	15.	单笔交易限额	2	单次交易的最大限额，由发卡/发码机构定义。	B
	16.	用户公钥	33	用户公钥数据（发码机构动态创建）	B
	17.	发码机构保留数据长度	1	发码机构保留数据的长度	B
	18.	发码机构保留数据	依赖表3.17	由发码机构自行定义	B
	19.	发码机构授权过期时间	4	发码机构授权失效时间，确保用户一定时间内离线使用码源（发码机构设定）	B Unix时间戳，对应1970的时间差 例如： 1505140363 表示 2017/9/11 22:32:43 单位秒
	20.	发码机构授权信息签名	64	参与签名的数据： 表3中的第1-19项	B 编码格式RS
脱机数据	21.	二维码批次号	2	脱机二维码产生的批次码 00 - 表示联机产生 XX - 表示当前的脱机码的批次（从01开始，每产生一次顺序加1）	N
	22.	二维码生成时间	4	二维码生码的时间，单位秒	B Unix时间戳，对应1970的时间差 例如： 1505140363 表示 2017/9/11 22:32:43 单位秒
	23.	用户脱机数据签名	64	参与签名的数据： 表3中第1-22项	B
注：BCD格式编码的数据项，采用后补‘F’。					

6.5 二维码的验证

受理终端读取二维码信息进行验证，流程见图5。

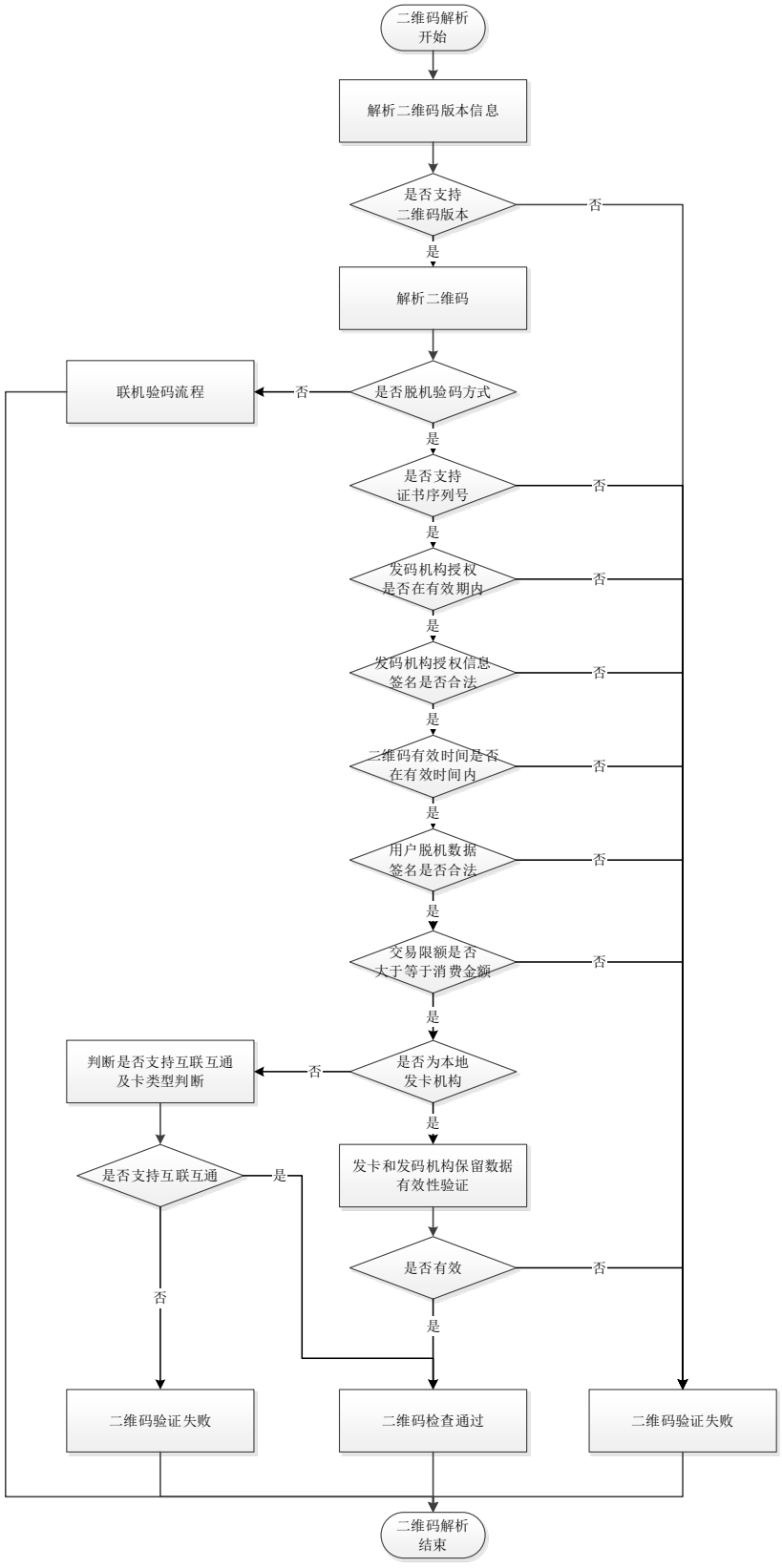

图5　二维码验证流程

二维码验证流程应符合下列要求：

a) 判断码源基本属性：检查二维码标识、版本信息和验码方式；
b) 确定码源合法性：检查发卡机构证书编号是否正确，验证发码机构授权是否在有效期内，用机构公钥验证发码机构授权信息签名是否合法；
c) 验证码源正确性：检查二维码是否在有效期内，验证用户脱机数据签名是否正确，保证内容不被破坏；
d) 验证二维码风险性：判断交易金额是否超出限制。

二维码检查通过后，受理终端将根据码源的机构属性及发卡/发码机构保留数据，选择执行本地或异地交易流程。交易成功后受理终端将生成交易记录，提示交易成功，并为用户提供乘车服务。

6.6 二维码的合法性

6.6.1 安全性保证

二维码的安全性保证由发卡机构私钥和用户私钥双重签名保证。二维码数据中发码机构授权信息签名信息需包含用户公钥信息，防止用户公私钥对的伪造。

6.6.2 实时性保证

二维码的实时性由联机数据中的‘二维码有效时长’及脱机数据中的‘二维码生成时间’保证，二维码客户端与受理终端均采用世界标准时间，应按以下方式保证时间同步：

a) 二维码客户端应具备定期或必要时与应用后台完成时间同步的机制，保证二维码客户端的生码时间与世界标准时间保持一致；
b) 受理终端应具备定期或必要时与收单机构后台系统完成时间同步的机制，保证受理终端在验码时效性。

7 交易记录转发

7.1 转发流程

使用城市智慧卡二维码完成交易时，用户需要在第一时间了解交易的执行状况。因此，脱机交易数据需准实时的通过云平台和发卡机构同步至发码机构，并转发给用户。对于复合交易，需要合并生成一条交易记录再进行转发。交易记录转发流程见图6。

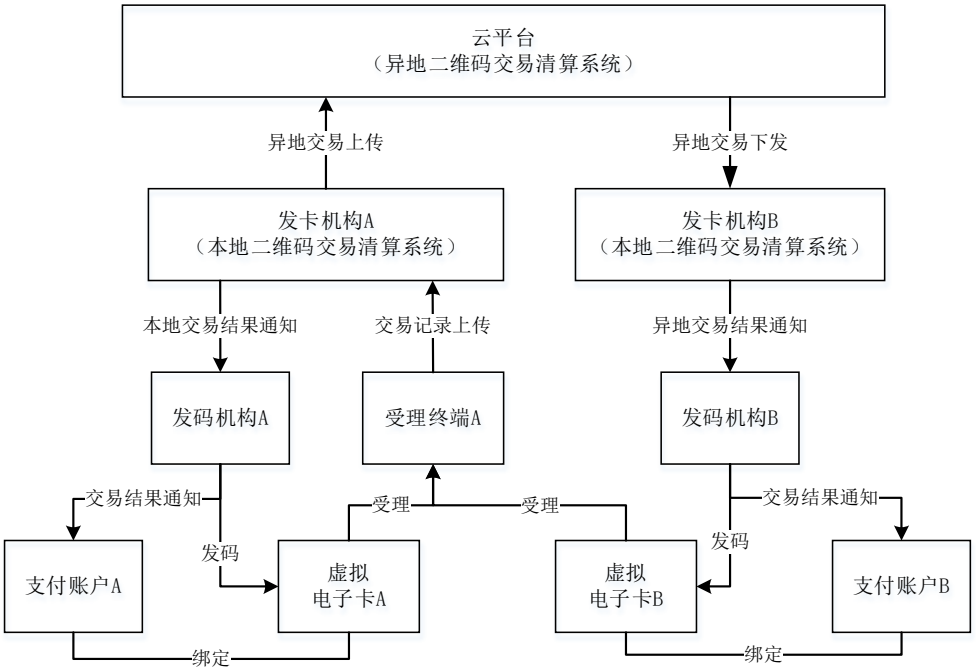

图6　交易记录转发流程

7.2　交易记录上传

7.2.1　用途

用于规范发卡机构到云平台的异地交易记录上送过程中的数据格式。

7.2.2　请求内容

交易请求内容符合表4的规定。

表4　交易记录上传请求内容

序号	字段名称	长度	格式	数据来源	描述
1.	上传请求时间	10	N	上传机构	上传交易的发卡机构上传交易记录请求时间（基准 1970-01-01） 例如：1505140363 表示 2017/9/11 22:32:43
2.	上传机构代码	15	N		云平台分配给上传交易的发卡机构的唯一识别码
3.	上传日期	8	N		YYYYMMDD
4.	上传机构流水号	12	N		上传交易的发卡机构上传操作流水号，上传日期和上传机构流水号确定上传操作的唯一性
5.	发卡机构代码	15	N	收单系统	来自二维码数据

6.	发码机构代码	15	N		来自二维码数据
7.	电子卡号	20	N		来自二维码数据
8.	交易日期	8	N		收单处理日期（YYYYMMDD）
9.	交易时间	6	N		收单处理时间(HHMMSS)
10.	交易金额	12	N		收单实扣金额(单位为分)优惠信息。
11.	原始金额	12	N		收单标定金额(单位为分)
12.	收单机构代码	15	N		收单机构代号，由发卡机构定义。
13.	收单系统流水号	12	N		收单交易流水
14.	交易类型	1	N		单次交易或复合交易
15.	原始二维码条数	1	N		交易原始二维码信息条数
16.	POS 信息 1	12	ANS		第 1 条 POS 信息 其中厂商编号 2 字节， POS 编号 6 字节 POS 交易流水号：4 字节
17.	原始二维码信息 1 长度	2	N		第 1 条原始二维码信息长度
18.	原始二维码信息 1	依赖表 4.17	N		第 1 条原始二维码信息
19.	…				第 2 条至第 n-1 条原始二维码长度及信息
20.	受理终端信息 n	12	N		第 n 条 POS 信息 其中厂商编号 2 字节， POS 编号 6 字节 POS 交易流水号：4 字节
21.	原始二维码信息 n 长度	2	N		第 n 条原始二维码信息长度
22.	原始二维码信息 n	依赖表 4.21	N		第 n 条原始二维码信息
23.	乘车信息	512	ANS		对于乘车信息 包含： 线路： 上车时间 下车时间 上车站点 下车站点 上传内容为 JSON 字符串 例如：

					{“line”：“北京1路”}
24.	签名数据	64	N		机构私钥或转发机构私钥对所有数据项签名（表4中1-23项）
注：本表格中上传机构指上传交易记录的发卡机构。					

7.2.3 响应内容

交易记录上传响应格式符合表5的规定。

表5 交易记录上传响应格式

序号	字段名称	长度	类型	描述
1.	响应代码	4	N	0000 - 成功 其他 - 失败
2.	错误描述	64	ANS	UTF-8格式编码
3.	上传机构代码	15	N	云平台分配给上传交易的发卡机构的唯一识别码
4.	上传日期	8	N	YYYYMMDD
5.	上传机构流水	12	N	上传交易的发卡机构上传操作流水号。上传日期和上传机构流水号确定上传操作的唯一性
6.	云平台日期	8	N	YYYYMMDD
7.	云平台流水号	12	N	云平台给此事件的流水号。
8.	签名数据	64	N	CA私钥对所有数据项签名（表5中1-7项）
注：本表格中上传机构指上传交易记录的发卡机构。				

7.3 交易记录下发

7.3.1 用途

用于规范云平台到发卡机构的异地交易记录下发过程中的数据格式。

7.3.2 请求内容

交易记录下发请求格式符合表6的规定。

表6 交易记录下发请求格式

序号	字段名称	长度	格式	数据来源	描述
1.	云平台代码	15	N	云平台	云平台的唯一编码
2.	云平台请求日期	8	N		YYYYMMDD
3.	云平台请求时间	10	N		云平台的请求时间 请求时间（基准1970-01-01） 例如：1505140363

					表示：2017/9/11 22:32:43
4.	云平台流水号	12	N		云平台给此事件的流水号，云平台日期和云平台流水号来确定交易的唯一性
5.	上传机构代码	15	N	上传机构	云平台分配给上传交易的发卡机构的唯一识别码
6.	上传日期	8	N		YYYYMMDD
7.	上传机构流水号	12	N		上传交易的发卡机构上传操作流水号，上传日期和上传机构流水号确定上传操作的唯一性
8.	发卡机构代码	15	N	收单系统	来自二维码数据
9.	发码机构代码	15	N		来自二维码数据
10.	电子卡号	20	N		来自二维码数据
11.	交易日期	8	N		收单处理日期（YYYYMMDD）
12.	交易时间	6	N		收单处理时间(HHMMSS)
13.	交易金额	12	N		收单实扣金额(单位为分)，针对优惠信息。
14.	原始金额	12	N		收单标定金额(单位为分)
15.	收单机构代码	15	N		交易发生地收单机构代码
16.	收单系统流水号	12	N		收单交易流水
17.	交易类型	1	N		单次或复合
18.	原始二维码条数	1	N		交易相关原始二维码信息条数
19.	POS 信息 1	12	ANS		第 1 条 POS 信息 其中厂商编号 2 字节， POS 编号 6 字节 POS 交易流水号：4 字节
20.	原始二维码信息 1 长度	1	N		第 1 条原始二维码信息长度
21.	原始二维码信息 1	依赖表 6.21	N		第 1 条原始二维码信息
22.	…	—	—		第 2 条至第 n-1 条原始二维码长度及信息
23.	POS 信息 n	12	N		第 n 条 POS 信息 其中厂商编号 2 字节， POS 编号 6 字节

					POS 交易流水号：4 字节
24.	原始二维码信息 n 长度	1	N		第 n 条原始二维码信息长度
25.	原始二维码信息 n	依赖表 6.25			第 n 条原始二维码信息
26.	乘车信息	512	ANS		对于乘车信息 包含： 线路： 上车时间 下车时间 上车站点 下车站点 上传内容为 JSON 字符串 例如： {“line”:”北京 1 路”}
27.	签名数据	64	N		CA 私钥对所有数据加密（表 6 中 1-26 项）
注：本表格中上传机构指上传交易记录的发卡机构。					

7.3.3 响应内容

交易记录下发响应格式符合表7的规定。

表7 交易记录下发响应格式

序号	字段名称	长度	类型	描述
1.	响应代码	4	N	0000 - 成功 其他 - 错误
2.	错误描述	64	ANS	UTF-8 格式编码
3.	上传日期	8	N	YYYYMMDD
4.	上传机构流水号	12	N	云平台给此事件的流水号，云平台日期和云平台流水号来确定交易的唯一性
5.	云平台日期	8	N	YYYYMMDD
6.	云平台流水号	12	N	云平台给此事件的流水号，云平台日期和云平台流水号来确定交易的唯一性
7.	发卡机构日期	8	N	YYYYMMDD
8.	发卡机构流水号	12	N	接收交易记录下发的发卡机构流水号，发卡机构日期和发卡机构流水号来确定交易的唯一性

9.	签名数据	64	N	发卡机构私钥或转发机构私钥对所有数据项签名（表 7 中 1-8 项）

7.4 通信方式

为满足发卡机构与云平台间交易记录转发的准时性要求，防止传输过程中的数据被截获或篡改，需对通信内容和通信方式进行安全保护，符合下列要求：

a) 通讯内容：交易记录数据的安全性由机构私钥的签名来保护，签名内容作为交易记录数据的一部分一并转发；
b) 通讯方式：采用加密方式的 HTTPS 传输方式来保证。

具体的交易记录转发通信方式如表8。

表8 交易记录转发通信方式

项目	说明
传输方式	采用加密的 HTTPS 协议 ，保证传输方式的安全性
提交方式	采用 POST 方法提交传输，保证提交方式的灵活性
数据格式	返回参数均为 JSON 格式，保证统一的通讯格式
字符编码	支持 UTF-8 字符编码，保证编码的通用性。
签名算法	对交易记录明文数据所有数据项用 SM2 算法做签名
签名要求	请求和接收数据均需要校验签名； 记录上传时，发卡机构使用机构私钥或转发机构私钥签名，交易记录下发时云平台使用 CA 私钥签名。

7.5 签名方式

7.5.1 签名密钥

签名密钥的生成方式如下：

a) 已经获取机构公钥证书的发卡机构：若发卡机构已经参与二维码联机数据的签名，具备机构公钥证书，上传交易记录过程中采用机构私钥对上传内容进行签名，交易记录下发过程中对收到的内容用 CA 公钥进行验证；
b) 未经获取机构公钥证书的发卡机构：若发卡机构未参与二维码联机数据的签名，不具备机构证书，则需向 CA 认证中心提交申请，生成交易记录转发公私钥对，由 CA 私钥签名生成专门的转发机构证书，用户交易记录转发过程中的数据签名。上传交易记录过程中采用转发机构私钥对上传内容进行签名，交易记录下发过程中对收到的内容用 CA 公钥进行验证。

7.5.2 数据签名

数据签名部分生成方式如下：

a) 生成请求参数字符串：对请求参数，即对交易记录转发文件的数据项排序，拼接出字符串 A；

b) 字符串的生成方式：将请求的非空参数按照参数名的 ASCII 码从小到大排序（字典序），使用 URL 键值对的格式即“key1=value1&key2=value2…”拼接成字符串 A；

c) 数据项的签名要求：

3) 参数名需要区分大小写，参数值为空的数据项不参与签名运算；

4) 参数名需按照 ASCII 码正序排列（字典序）；

5) 交易记录中的“签名数据”项，即请求或相应数据格式的最后一项不参与签名运算。

8 清分结算类文件

8.1 清算反馈文件（供收单机构使用）

8.1.1 用途

用于规范下发清分、清算记录。

8.1.2 命名规则

用于规范下发清分、清算记录。

表9 清算反馈文件命名规则

数据元说明	数据类型	长度	值
文件标识	A	2	AC
日期	N	8	YYYYMMDD
收单机构代码	N	15	000000000000001～999999999999999
序列号	N	6	000000～999999

8.1.3 文件格式

文件格式应符合表10的规定。

表10 清算反馈文件格式

数据元说明	数据类型	长度	备 注
文件说明区			
版本号	N	2	01
交易类型	N	4	值3000
回车符	S	2	0x0d和0x0a
交易头			
清算日期	N	8	YYYYMMDD
记录总数	N	8	取值范围为00000001～99999999
累计交易金额	N	12	取值范围为000000000001～999999999999(单位分)
应收金额	N	12	取值范围为000000000001～999999999999(单位分)
总佣金手续费	N	12	取值范围为000000000001～999999999999(单位分)

云平台总手续费	N	12	取值范围为000000000001～999999999999(单位分)
发码机构总手续费	N	12	取值范围为000000000001～999999999999(单位分)
收单机构总手续费	N	12	取值范围为000000000001～999999999999(单位分)
收单机构代码	N	15	000000000000001～999999999999999
单笔交易长度	N	4	包含回车换行：取值范围为0001～9999 （注：指交易数据体的字节长度总和，各机构上传数据单笔交易长度必须符合云平台标准）
保留域	ANS	8	全0
回车符	S	2	0x0d和0x0a
交易数据体			
云平台流水	N	12	取值范围为000000000001～999999999999 （注：云平台流水号）
收单流水号	N	12	取值范围为000000000001～999999999999 （注：由收单中心产生的交易流水号）注：如本地流水号小于12位时，前补0
电子卡号	N	20	取值范围为00000000000000001～FFFFFFFFFFFFFFFFFF
交易金额	N	8	取值范围为00000001～99999999
交易发生日期	N	8	YYYYMMDD
交易发生时间	N	6	HHMMSS
回车符	S	2	0x0d和0x0a

8.2 结算明细文件（供发卡机构使用）

8.2.1 用途

用于规范下发清分、结算记录。

8.2.2 命名规则

命名规则应符合表11的规定。

表11 结算明细文件命名规则

数据元说明	数据类型	长度	值
文件标识	A	2	IS
日期	N	6	000101～991231
发卡机构代码	N	15	000000000000001～999999999999999
序列号	N	6	000000～999999

8.2.3 文件格式

文件格式应符合表12的规定。

表12 结算明细文件格式

数据元说明	数据类型	长度	备　注
文件说明区			
版本号	N	2	01
交易类型	N	4	值4000
回车符	S	2	0x0d和0x0a
交易头			
清算日期	N	8	YYYYMMDD
记录总数	N	8	取值范围为00000001～99999999
累计交易金额	N	12	取值范围为000000000001～999999999999(单位分)
应付金额	N	12	取值范围为000000000001～999999999999(单位分)
总佣金手续费	N	12	取值范围为000000000001～999999999999(单位分)
云平台总手续费	N	12	取值范围为000000000001～999999999999(单位分)
发码机构总手续费	N	12	取值范围为000000000001～999999999999(单位分)
收单机构总手续费	N	12	取值范围为000000000001～999999999999(单位分)
单笔交易长度	N	4	包含回车换行：取值范围为0001～9999 （注：指交易数据体的字节长度总和，各地上传数据单笔交易长度必须符合数据云平台标准）
保留域	ANS	8	全0
回车符	S	2	0x0d和0x0a
交易数据体			
云平台流水	N	12	取值范围为000000000001～999999999999 （注：云平台流水号）
收单流水号	N	12	取值范围为000000000001～999999999999 （注：由收单中心产生的交易流水号）注：如本地流水号小于12位时，前补0
电子卡号	N	20	取值范围为00000000000000001～FFFFFFFFFFFFFFFFF
交易金额	N	8	取值范围为00000001～99999999
交易发生日期	N	8	YYYYMMDD
交易发生时间	N	6	HHMMSS
回车符	S	2	0x0d和0x0a

8.3　通信方式

云平台建立专门的清分结算服务器，用于存放发卡机构或收单机构的结算反馈文件和结算明细文件。

云平台对于批量的交易记录，采用T+1的方式进行清分结算处理，将产生的结算反馈文件和结算明细文件，上传至清分结算服务器中。对接入云平台的发卡机构、收单机构要求如下：

a)　云平台为接入机构提供接入设置，允许机构访问清分结算服务器；

b)　云平台为接入机构分配用户名和密码，同时分配访问权限，保证机构只能访问对应的清分结算信息。

c)　机构登录每日连接文件服务器，下载相应的文件。

9 住区二维码应用

9.1 系统要求

9.1.1 系统架构

住区认证二维码系统架构如图7所示。

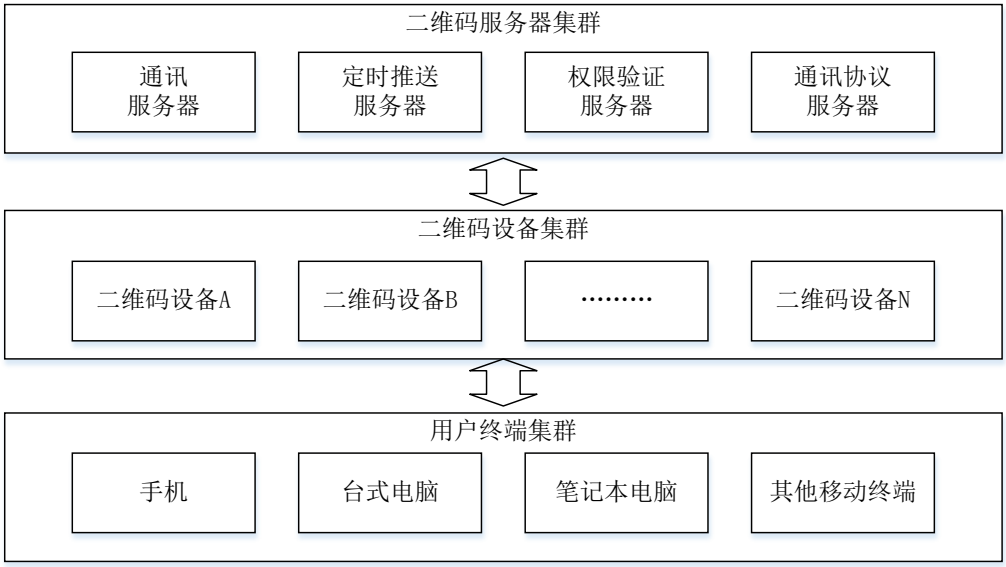

图7 住区认证二维码系统架构图

住区认证二维码系统由二维码服务器集群、二维码设备集群、用户终端集群三个部分组成，并符合下列要求：

a) 通讯服务器：用来存储二维码设备信息，并负责向二维码设备发出设置或控制指令；
b) 定时推送服务器:用来定时向二维码设备发送连接信号,保持服务器与二维码设备的必要链接，为时钟同步、权限同步等功能的提供支持；
c) 权限验证服务器：在主扫过程中用来接收并验证用户终端的权限，在被扫过程中向二维码设备下放必要的权限；
d) 通信协议服务器：用来储存、管理、维护二维码设备、用户终端与各服务器之间的通信协议；
e) 二维码设备：安装在门禁中的受理终端，在整体系统中起到验证的枢纽作用，建立用户终端与服务器的必要连接；
f) 用户终端应符合下列要求：
   6) 手机是用户住区二维码扫描时候的关键部件，用来显示二维码或扫描设备上的二维码；
   7) 台式电脑和笔记本电脑是提供给系统管理者使用的维护工具；
   8) 其他移动终端是能满足普通用户或管理者使用的其他移动设备，如平板移动终端、手持终端等。

9.1.2 业务流程

9.1.2.1 一般规定

住区二维码管理系统采用主扫和被扫两种不同认证方式，符合下列要求：

a) 主扫即用户通过手机主动扫描并验证门禁上二维码设备生成二维码，达到身份认证的目的；
b) 被扫即用户通过手机屏幕或纸质票证显示二维码，被门禁上二维码设备扫码并验证，达到身份认证的目的。

9.1.2.2 主扫

住区认证二维码主扫业务流程如图8所示。

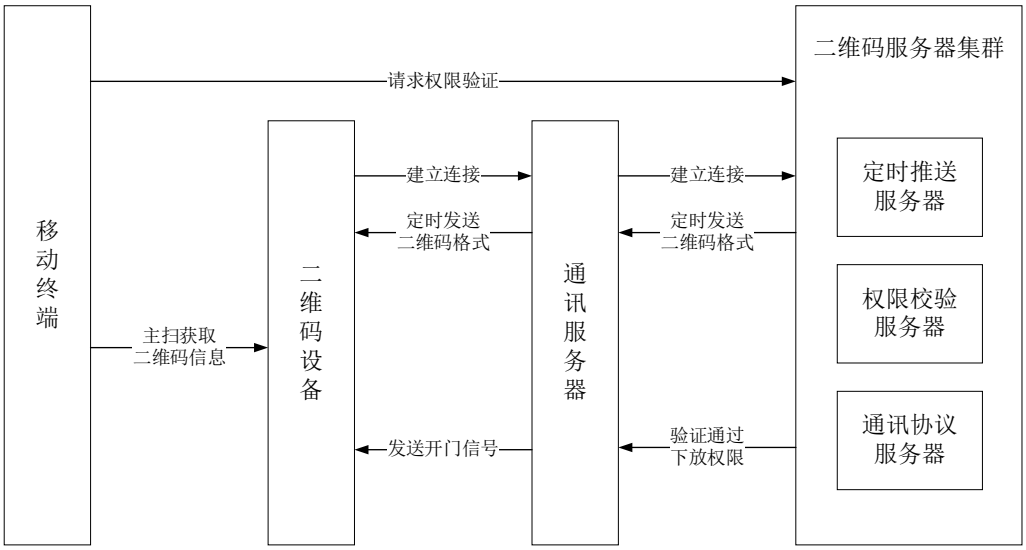

图8 住区认证二维码主扫业务流程图

住区认证二维码主扫业务流程说明如下：

a) 二维码设备在安装时，需与服务器建立连接，不用区域的二维码设备会连接不同的服务器，保证系统的稳定和容错性；
b) 服务器定时给二维码设备发送二维码内容，即实现二维码的自动或定时刷新，二维码格式参见表 13 描述的二维码数据结构；
c) 用户使用二维码客户端扫描二维码设备，将二维码信息进行本地验证或上传服务器进行验证；
d) 如手机脱机，则通过手机与二维码设备建立连接（如蓝牙等），发送开门指令；如手机联机，则通过服务器给二维码设备发送开门指令。对于权限不符合要求的用户提示认证失败。

9.1.2.3 被扫

住区认证二维码被扫业务流程如图9所示。

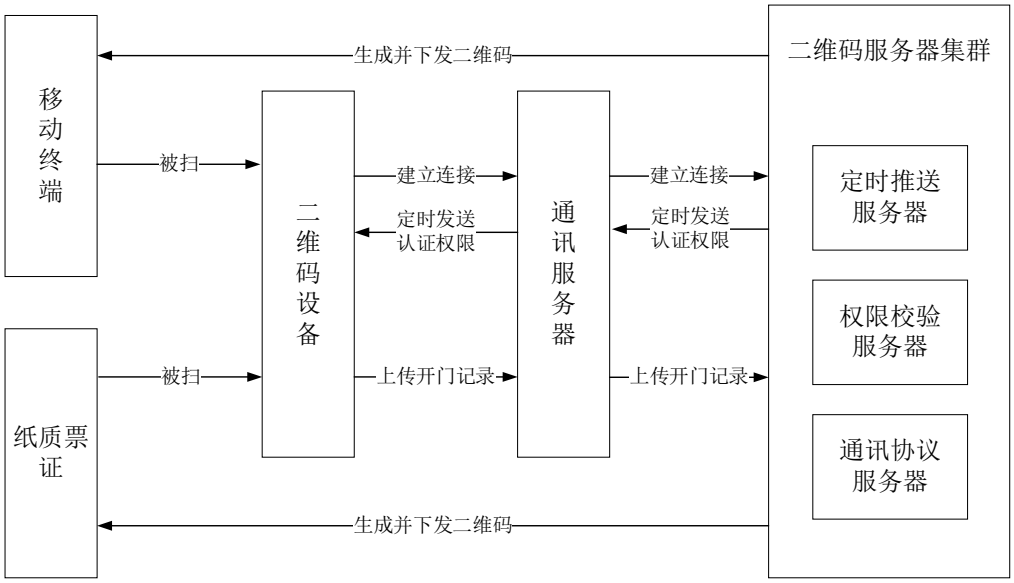

图9　住区认证二维码被扫业务流程图

住区认证二维码被扫业务流程说明如下：

a）　服务器向用户发放二维码，载体可以是手机二维码客户端或纸质票证，二维码包含用户的基本信息和用户权限信息；

b）　二维码设备扫描用户二维码，读取用户基本信息和权限信息，根据存储在设备中的认证权限对二维码信息进行判断。二维码设备会定时或必要时与二维码服务器进行权限信息同步；

c）　二维码设备执行命令后生成开门记录，通过通信服务器上传至服务器。

9.2　管理系统

9.2.1　交互模式

9.2.1.1　主扫交互模式

主扫交互模式示意图如图10所示，并应符合下列要求：

a）　用户使用二维码客户端扫描主扫二维码设备显示的二维码，获取二维码包含的信息内容；

b）　二维码客户端进行脱机验证或联机将用户信息及获取到的二维码信息上传至服务器进行验证；

c）　若采脱机验证，通过手机与二维码设备进行连接（如蓝牙等），将开门指令至二维码设备；若采用联机认证，服务器验证用户权限信息后下发开门指令至二维码设备；

d）　二维码设备执行开门指令，并返回执行成功后结果至服务器；

e）　服务器将本次操作结果返回至手机二维码客户端进行显示。

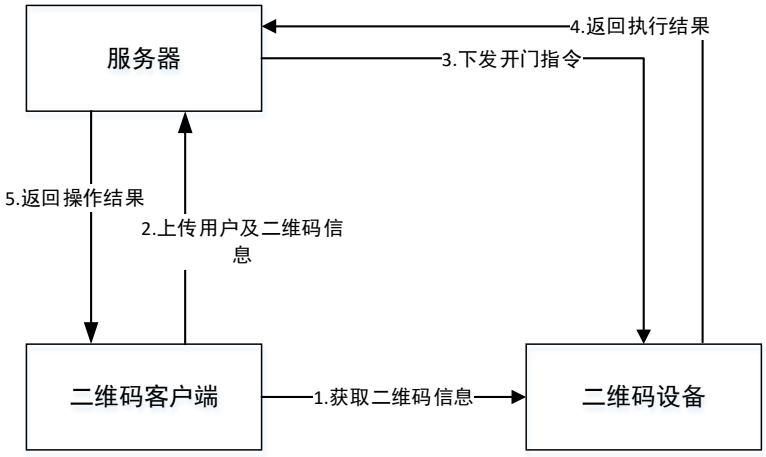

图10　主扫交互模式示意图

9.2.1.2　被扫交互模式

9.2.1.2.1　一般规定

被扫交互模式下，二维码包含业主码和访客码两种类型。

被扫交互模式示意图如图11所示，并应符合下列要求：

a)　用户将二维码客户端或纸质票证上显示的二维码被二维码设备扫描并获取二位信息；

b)　二维码设备根据识别到的内容进行权限判断，下发开门指令；

c)　二维码设备将开门记录上传至服务器。

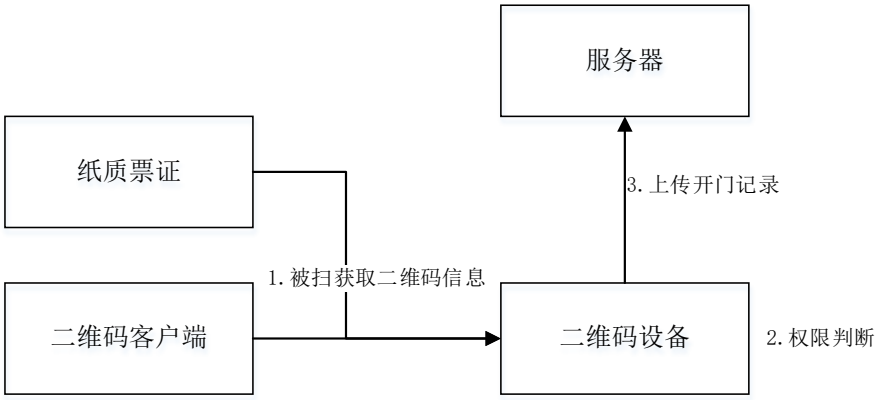

图11　被扫交互模式示意图

9.2.1.2.2　业主码

业主码供住区业主所有，属长期使用的二维码，码源权限信息存储至手机设备中，权限信息较丰富，安全性较高。在业务码的使用过程中，服务器向用户发放业主码，业主码中包含用户的唯一识别码。同时业主的权限信息将下载至二维码设备中，由二维码设备进行存储，用户扫码时，二维码设备读取用户唯一识别码，搜索设备内已保存的权限信息进行判断。

业主码发放需要服务器与二维码设备进行通讯，权限信息由二维码设备存储以保证安全性和稳定性。

9.2.1.2.3 访客码

访客码供临时访客所有，属临时使用的二维码，权限信息储存在二维码中，使用更加便捷。在访客码的使用过程中，服务器向用户发放访客码，访客码包含用户的唯一识别码和用户权限信息。用户扫码时，二维码设备读取用户唯一识别码和权限信息，进行权限判断。

访客码发放不需要与二维码设备进行通讯，权限存储在二维码内，数据量较少，认证更加便捷。

9.2.2 密钥管理

住区认证二维码采用HTTPS协议传输，包含SM4对称加密算法和SM2非对称加密算法保证数据安全。密钥机制如图12所示。

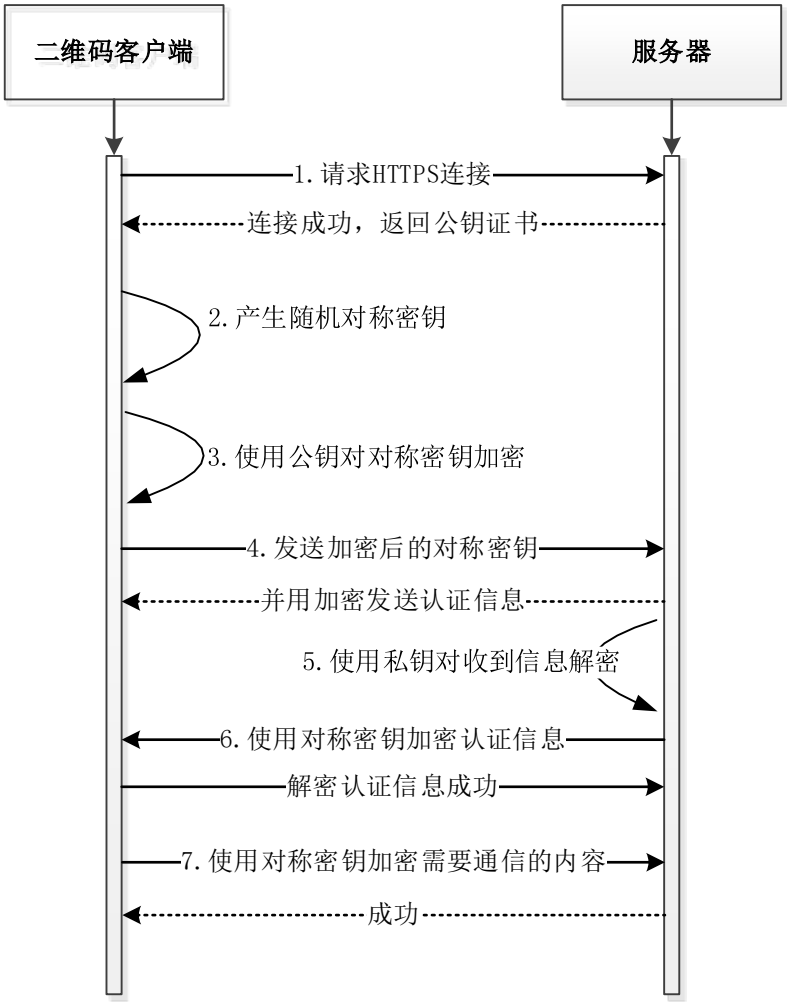

图12 住区认证二维码密钥管理

并应符合下列要求：

a) 二维码客户端将向服务器请求 HTTPS 连接，服务器端产生非对称公私钥对，并将公钥以证书的形式发送给二维码客户端；

b) 二维码客户端获得服务器证书之后，二维码客户端会随机生成对称密钥，用于后续传输中的数据加密；

c) 二维码客户端使用服务器证书中提供的公钥将随机对称密钥进行加密；

d) 二维码客户端将加密后对称密钥发送给服务器，服务器接收客户端发来的密文后，使用私钥解密取出对称密钥；
e) 服务器使用对称密钥加密一段认证信息并发送给二维码客户端；
f) 二维码客户端解密认证信息，此时互认证结束；
g) 后续，通信数据将由此次二维码客户端生成的随机对称密钥加密传输。

9.2.3 二维码数据组成

住区二维码数据分为主扫模式和被扫模式，其中主扫模式中，根据手机是否联机，二维码可分为联机二维码和脱机二维码两种情况；被扫模式中，仅脱机数据，住区二维码数据结构见表13。

表13 住区二维码数据结构

模式	类别	序号	字段名	长度	描述	格式
主扫模式	联机二维码	1.	发码机构标志	3	住区二维码发码机构的标识号	B
		2.	标签类型	2	判断标签的分类	B
		3.	住区唯一标记	6	判断住区之间的唯一标记	B
		4.	设备唯一编号	16	每个硬件设备的唯一通信识别号	B
		5.	随机密钥	4	每次与后台通信，需验证随机密钥	B
		6.	发码时间	8	根据服务器生成时间发放（日时分秒）	B
	脱机二维码	7.	发码机构标志	3	发码机构标志	N
		8.	设备唯一编号	16	每个硬件设备的唯一通信识别号	B
被扫模式	脱机数据	1.	二维码产生时间	4	起始为 1970.1.1 的时间戳	B
		2.	随机密钥	4	用于加密计算	B
		3.	发码机构标志	2	住区二维码发码机构的标识号	B
		4.	用户唯一标记	8	每个用户的唯一识别码	B
		5.	有效时间	6	超过有效时间，将失去权限	B
		6.	门禁块	16	‘A’（1B）、数量（1B）、【编号+门位】×7；	B
		7.	梯控块	32	‘T’（1B）、数量（1B）、【编号+层数+楼层×M】×8	B
		8.	访客块	16	‘F’（1B）、限出分钟（2B）、数量（1B）、【编号】×12	B
		9.	CRC	2	对通用块到访客块明文数据进行 CRC 计算	B
		10.	SUM	2	对 SUM 前面每字节数据进行求和计算	B

9.2.4 二维码的验证

9.2.4.1 主扫验证

住区二维码主扫验证流程如图13所示，并应符合下列要求：
a) 用户使用二维码客户端扫描二维码设备显示的二维码；
b) 如果手机处于脱机状态，二维码客户端采用预先储存的认证权限进行脱机认证，认证通过后使用手机与二维码设备通过一定方式通讯（如蓝牙），发送开门指令；
c) 如果手机处于联机状态，二维码客户端将用户信息及二维码信息上传至服务器进行验证；

d) 服务器验证用户权限信息后下发开门指令至二维码设备。

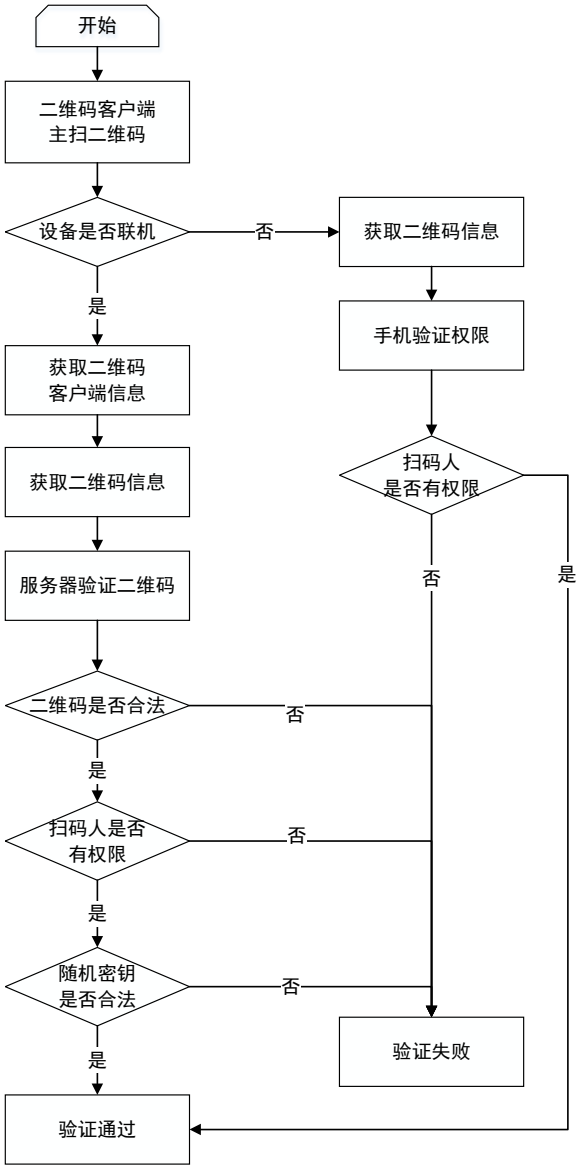

图13 住区二维码主扫验证流程

9.2.4.2 被扫验证

住区二维码被扫验证流程如图14所示，并符合下列要求：

a) 用户将二维码客户端或纸质票证上显示的二维码，被二维码设备扫描，获取二维码信息；

b) 二维码设备脱机验证用户唯一识别码，判断用户身份；

c) 二维码设备验证二维码时间是否有效、合法；

d) 二维码设备验证二维码数据中的块类型、块内数据、随机密钥等是否合法；

e) 验证通过后，二维码设备生成开门指令。

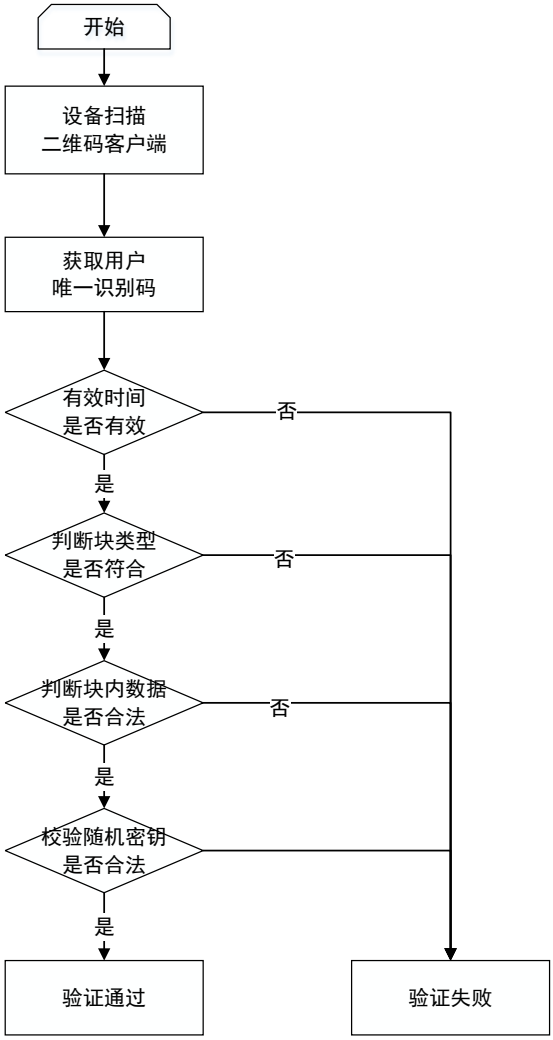

图14　住区二维码被扫验证流程

9.3　通信要求

二维码设备与服务器通过UDP协议进行通讯，可选择使用有线和WIFI无线等方式；

二维码客户端与服务器通过HTTP协议进行通讯，可选择使用3G/4G移动蜂窝网络和WIFI无线方式。

附 录 A
（规范性附录）
互联互通标志

A.1 标志功能

互联互通标志用于区分和标识城市智慧卡二维码领域的相关产品及服务是否具备互联互通功能。

A.2 标志图样

A.2.1 互联互通标志

互联互通标志图样应符合图A.1的规定。

注：本图为互联互通标志的网格制图，每一个网格代表一个基本的计量单元，并用a表示。

图A.1 互联互通标志图样

A.2.2 参数

互联互通标志参数应符合下列要求：

a) 互联互通标志以白色为背景，衬托出蓝色的“CU”文字变形和红色的“City Union”造型，“City Union”字体为Georgia；
b) 互联互通标志的防伪标志为围绕在主题造型周围的42个“City Union”字样构成，字体为Georgia；
c) 互联互通标志的尺寸宽度为41a，高度为27a；
d) 四色印刷中蓝色标准色为C:100 M:20 Y:0 K:0，红色标准色为C:0 M:100 Y:100 K:10。