基于隐私保护的匿名码

技术方案

文件状态: [√] 草稿文件 [ ] 正式文件 [ ] 更改正式文件	文件编号	
	版　　本	V1.4
	作　者	张斌
	完成日期	
	保密级别	[ ] 特级 严格控制传阅 [ ] 一级 内部受控传阅 [√] 二级 内部传阅 [ ] 三级 流通

宁波市民卡运营管理有限公司信息科技部

2024-11-14

历史修改记录

编号	修改日期	版本号	修改说明	修改人	审核人
1	20240926	V1.0	初稿	张斌	
2	20241011	V1.1	增加了对于强隐私保护流程的处理	张斌	
3	20241107	V1.2	调整了请码流程、扣款流程的部分内容	张斌	
4	20241112	V1.3	增加了钱包备份，恢复流程，调整了开通流程	张斌	
5	20241114	V 1.4	增加了钱包余额退款，钱包关闭流程，调整了开通流程	张斌	

目 录

一、建设总体原则 4
二、技术实现方案 4
2.1 业务执行总体流程 4
2.2 匿名码开通流程 6
2.3 匿名码充值流程 6
2.4 匿名码请码流程 8
2.5 匿名码脱机扫码扣款流程 9
2.6 匿名码交易查询流程 10
2.7 匿名码违规追踪流程 11
2.8 匿名钱包余额返充 12
2.9 本地钱包数据备份 13
2.10 本地钱包数据恢复 14
2.11 匿名钱包余额退款 15
2.12 匿名钱包关闭 16
三、数据库设计 17
3.1 用户匿名钱包账户表 (ANONYMOUS_WALLET_ACCOUNTS) 17
3.2 用户 ID 对应记录表（USERID_RECORDS） 18
3.3 认证交易记表 certification_TRANSACTIONS 18
3.3 钱包交易记录表（Wallet_Transactions） 18
3.4 匿名码开通信息表（anonymous_code_user_relationship） 19
3.5 钱包余额返充登记表（purse_Refund_record） 19
四、系统部署架构 20
五、改造任务分工 20
六、改造时间安排 20

基于隐私保护的匿名码技术方案

根据公司“2035 科创甬江”关键技术突破计划的建设要求，需要完成用户隐私数据保护关键技术的应用落地。目前市民卡公司已经建成了基于乘车码的用户开户、扫码支付、清结算的技术平台，为配合用户隐私保护技术在乘车码应用中的落地实施，需要对乘车码平台的技术方案、实现流程做相关的技术改造，以满足用户在乘车码交易过程中用户行踪不可追踪以及隐私保护的要求。

一、建设总体原则

1、 保持原有乘车码主体流程不变，通过外部调用的方式增加隐私保护的认证以及相关数据的存储；
2、 二维码平台后端通过参数配置的方式增加匿名码类型，根据码类型确定后端的业务实现流程；
3、 APP 端开发新的匿名码入口模块，匿名码模块包括开通、展码、充值、记录查询 4 个子模块；
4、 APP 后端配置匿名码授权开通用户清单，可以实现单个、多个、或全部开通的配置。前端通过白名单授权方式确定用户对匿名码模块是否可见；
5、 APP 前端通过 SDK 调用方式实现相关的匿名数据认证，认证 SDK 与隐私后台独立交互；
6、 匿名码相关的隐私保护数据存储单独建表，匿名码开通的个人数据采用加密方式存储，开通记录表保存云卡卡号，加密方式采用SM4加密，密钥可配置；

二、技术实现方案

2.1 业务执行总体流程

基于隐私保护的乘车码、匿名码融合系统实现的功能主要包含码的开通、码账户充值、请码、交易记录查询、扫码扣款、违规行为的匿名追踪等功能。系统改造以市民卡公司原

有二维码平台为基础，通过新建隐私保护 SDK，隐私保护后台，改造开通、请码、扫码扣款接口实现乘车码、匿名码并行且功能模块独立的要求。各业务系统的执行流程如下图所示：

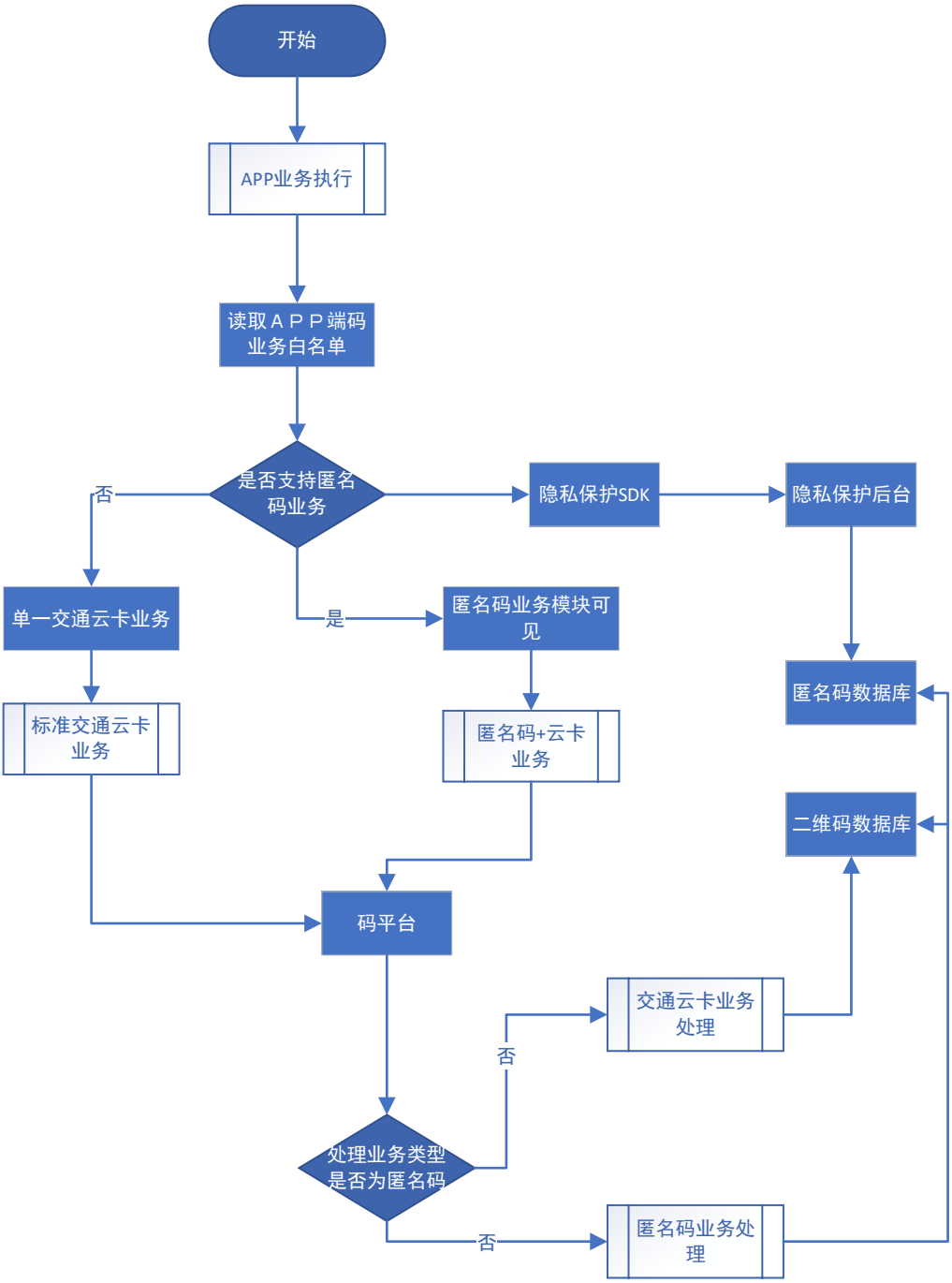

图 1：业务执行（支持匿名码）流程图

2.2 匿名码开通流程

匿名码开通依托于原交通云卡开通作交易主流程，APP 端在用户开通乘车码时，根据配置白名单判断是否可见匿名码入口，对于白名单内容的用户需要开通匿名码时，进入匿名码开通模块，APP 通过隐私保护 SDK 获取匿名开通的用户 userid，隐私保护后台根据开通请求首先在后台建立 userid 和只是承诺 J 的对应关系记录，码平台在收到匿名码开通请求时，首先查询是否存在认证记录，当存在时，通过读取配置信息，完成匿名码账户开通并单独加密保存开通记录，具体流程见图 2.

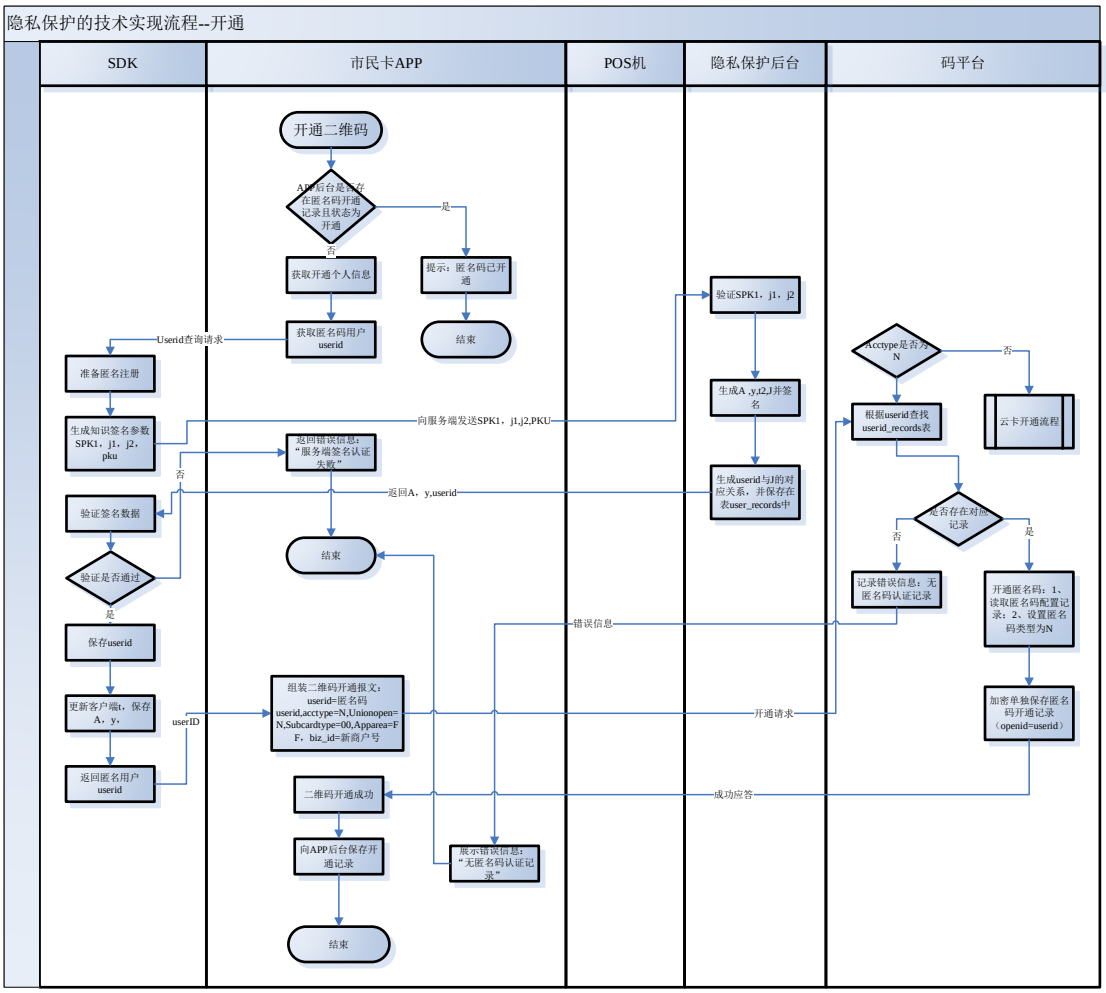

图 2：匿名码开通流程

2.3 匿名码充值流程

APP 端要进行匿名码账户充值，首选进入匿名码账户充值入口，通过调用匿名码 SDK 获

取匿名码账户账号信息 B1 和Ｂ，ＳＤＫ收到请求后，首先需要判断是否首次充值，如果首次充值则置Ｂ１＝０，否则Ｂ１＝匿名钱包原账号Ｂ，然后向隐私保护后台申请 challenge，通过 challenge 并结合本地参数向服务端发起合法性认证，如果对 SN 以及签名的认证通过则下发更新参数 A，y，并保存认证记录，SDK 收到参数后，更新客户端本地参数并将 B1，B 的值返回给 APP，APP 收到应答后，组装充值报文，码平台后端根据账户类型 acctype 判断是否匿名码充值，如果不是则走普通云卡充值流程，如果是则判断是否匿名码首次充值，如果首次充值则直接在匿名钱包账户表插入一条钱包账户记录并更新账户余额，在钱包交易记录表保存充值记录；如果不是首次充值，则需要根据 B1 的值从匿名钱包账户表找到一条账户记录，获取原账户余额，并生成一条新的账户记录，账户余额为原余额+充值金额，原账户记录置为注销状态。具体流程见图 3.

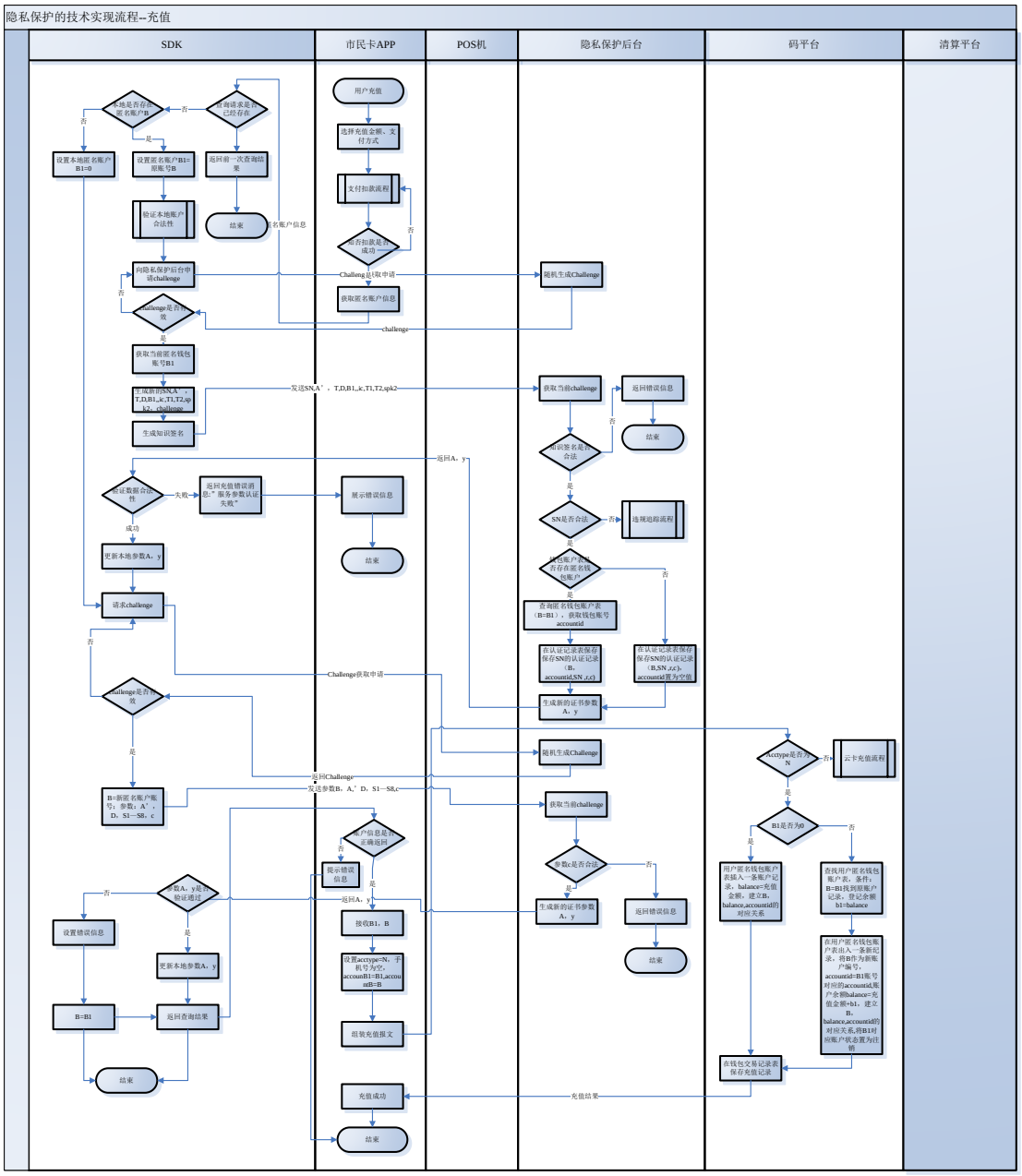

图 3：匿名码充值流程

2.4 匿名码请码流程

APP 端通过白名单授权进入匿名码请码界面，匿名码请码时，通过匿名 SDK 完成客户端的合法性认证并获取客户端的匿名钱包账户 sequence（nm+14 位不重复序列号），APP 组装请码报文，设定请码类型为匿名码 N，码平台根据请码报文中 acctype 判断是否为匿名码请码，如果不是匿名码则走普通云卡请码流程，否则走匿名码请码流程，匿名码请码时码平台首先根据 sequence 查询认证记录表，如果没有认证记录则报错，如果存在则根据 sequence 找到认证记录并获取账户 accountid,然后根据 accountid 查询匿名钱包账户表，

判断是否有开户记录，如果存在则将 16 位 sequence 值作为支付账号，将 accountid 作为用户账户号，账户类型保持原有云卡账户类型不变，组装二维码数据并保存请码记录。具体流程见图 4。

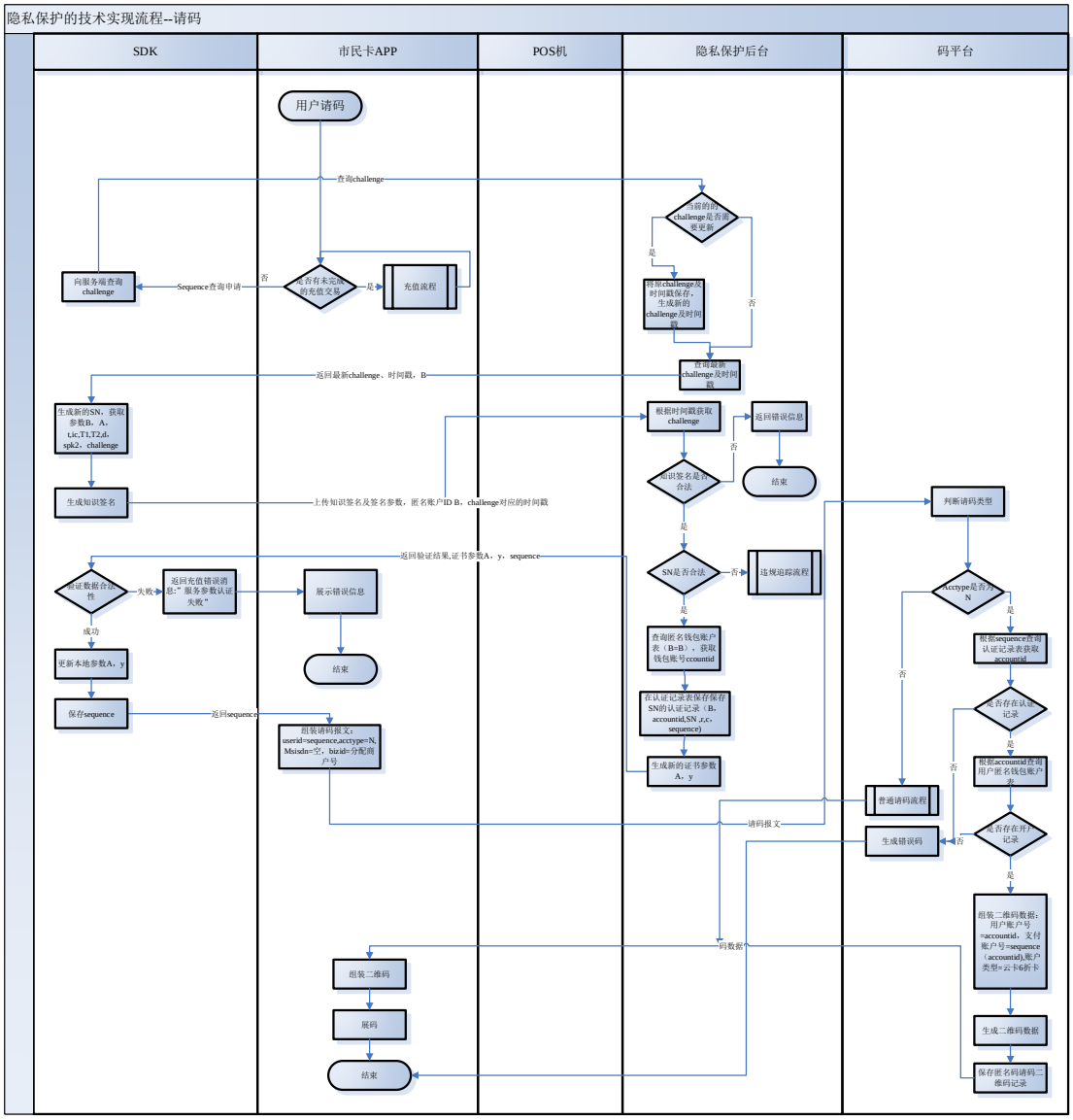

图 4：匿名码请码流程

2.5 匿名码脱机扫码扣款流程

POS 机扫码后验证二维码的真伪，验证通过后在本地保存并上送到 POS 前置，前置在识别交易数据为二维码数据后将明细数据发送到二维码平台，码平台根据获取二维码数据中的 bizid 值判断是否为匿名码商户发生的交易，如果不是则直接走云卡扣款流程；如果是

匿名码交易，首先根据码数据中的支付账户号和云卡卡号查询认证记录表，检查匿名码的请码记录的 SN 是否被使用，如果已经使用，则表示该二维码存在复制风险，记录日志信息，并扣减匿名钱包账户余额，保存钱包扣款记录、乘车记录；如果 SN 未被使用，则将 SN 对应的请码记录置为使用标记，并扣减匿名账户钱包余额，保存钱包交易记录、乘车记录；对于匿名钱包账户的状态已经设置为注销状态或余额不足的（为 0 或负数），也需要减相关的匿名钱包账户余额具体流程见图 5。

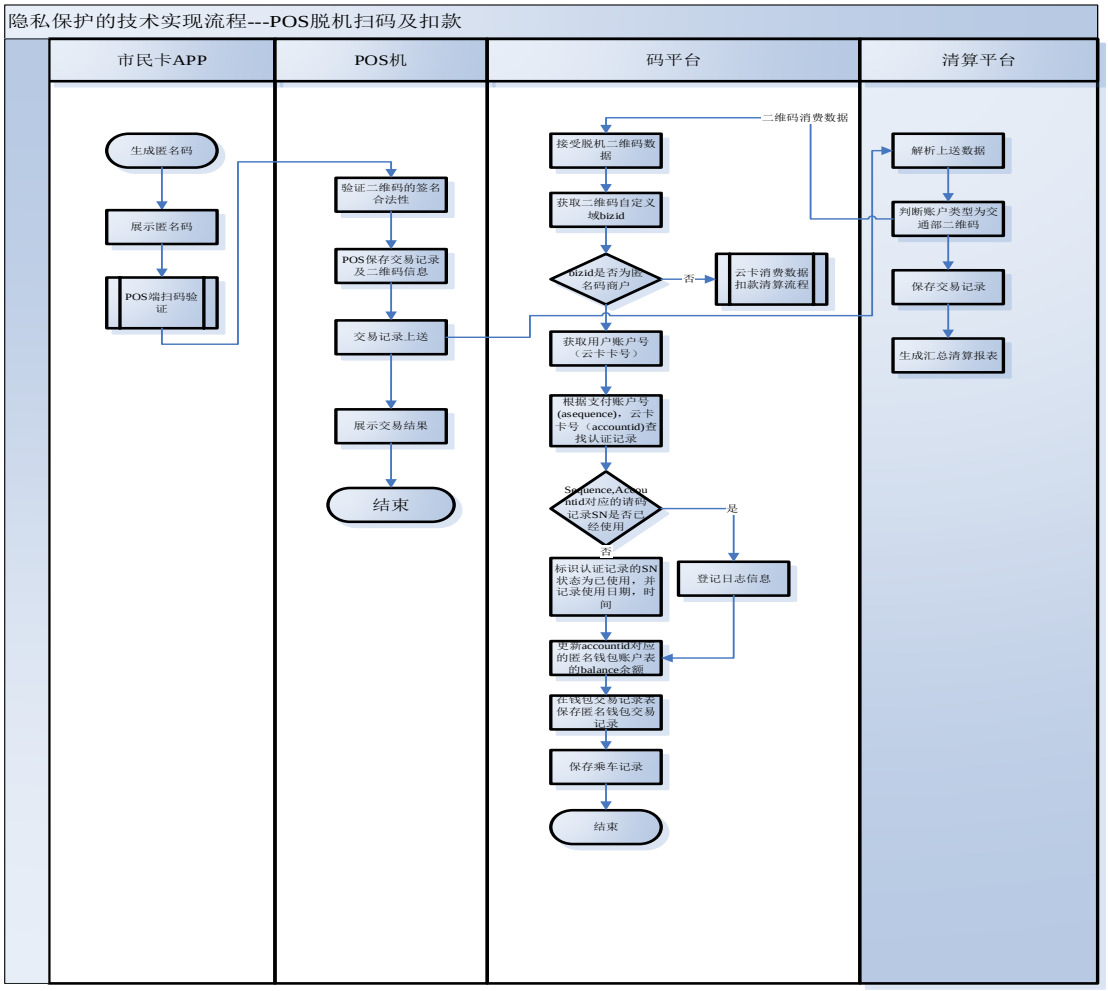

图 5：匿名码扫码扣款流程

2.6 匿名码交易查询流程

APP 端进入匿名码业务入口，向 SDK 发起 accountid 查询请求，对于匿名码查询需要区分充值交易查询和乘车记录查询并根据不同的类型组装相关报文。码平台收到请求后，首先判断是否匿名码查询报文，如果是则判断查询交易类型，根据交易类型从钱包交易记录表中查询指定的交易记录。如果是消费记录查询，则在查询到钱包消费交易记录后，还需

要根据 accountid 从乘车记录表中查询乘车记录信息，两者关联后，合并返回给 APP 端，具体的流程见图 6.

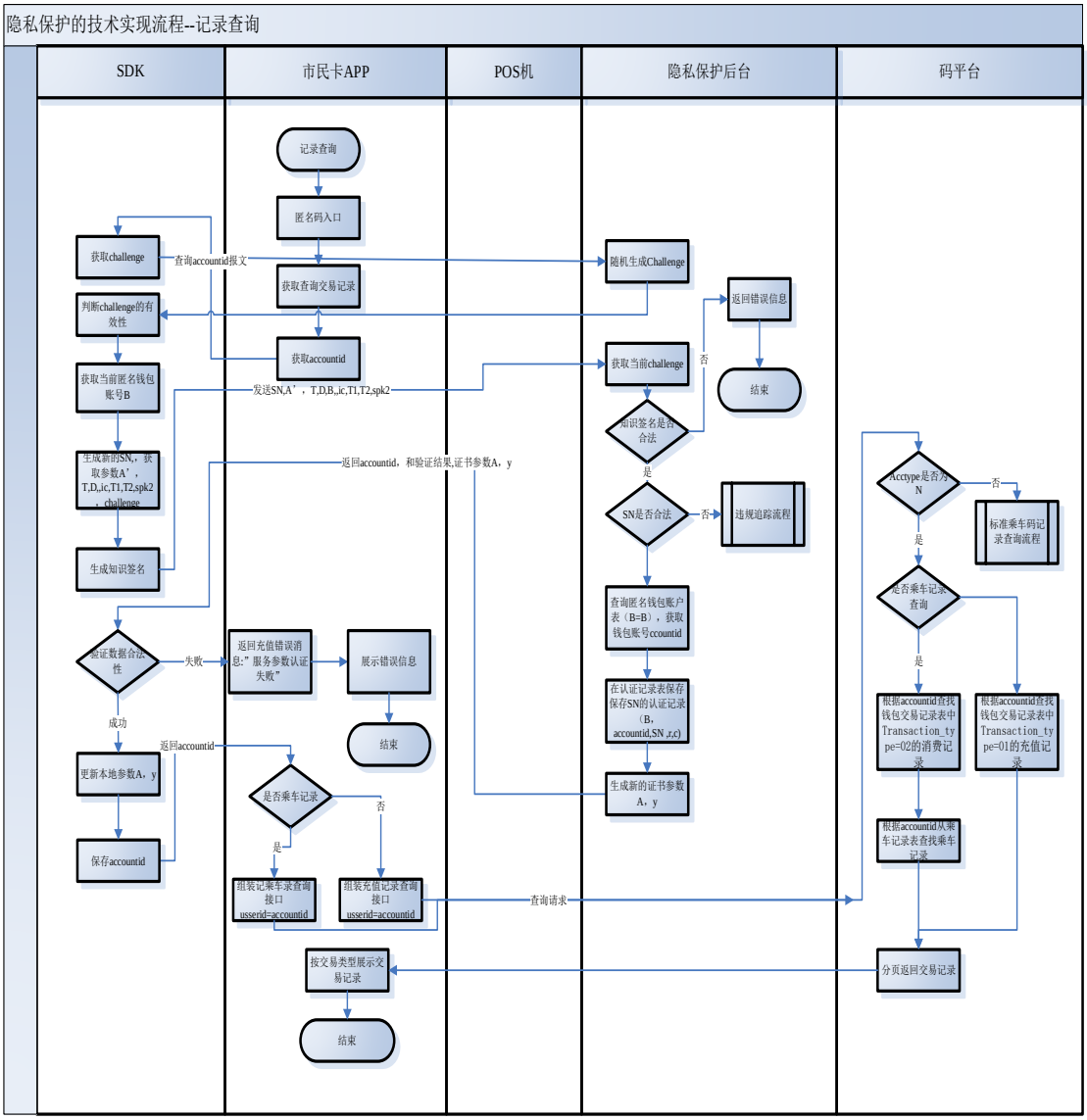

图 6：匿名码交易查询流程

2.7 匿名码违规追踪流程

客户端在完成充值、请码、交易记录查询过程中，会通过 SDK 向后端验证认证序列号 SN 的合法性，隐私保护后台在认证通过后会向客户端下发新的证书参数。当认证不通过时（SN 已经被使用），则判断客户端存在被克隆的风险，隐私保护后台会根据上送的被判定为存在风险 SN 与正常 SN 的参数计算出知识承诺 J，隐私保护后台根据 J 查找用户 ID 对应

记录表，找到 J 对应的 userID ，并根据上送的 B 查找对应的匿名钱包账户记录，将查询到的违规用户的 userid 更新到对应字段。

用户通过后管页面查询违规用户信息，系统查询匿名钱包账户记录表中 userid 不为空的记录即为标记为违规的匿名钱包账户记录，根据 userid 查询出对应的用户开通信息，根据 accountid 查询出匿名钱包交易表中的所有的充值记录和消费记录，完成对匿名用户的违规追踪以及该用户所有交易记录的溯源。具体流程见图 7 所示。

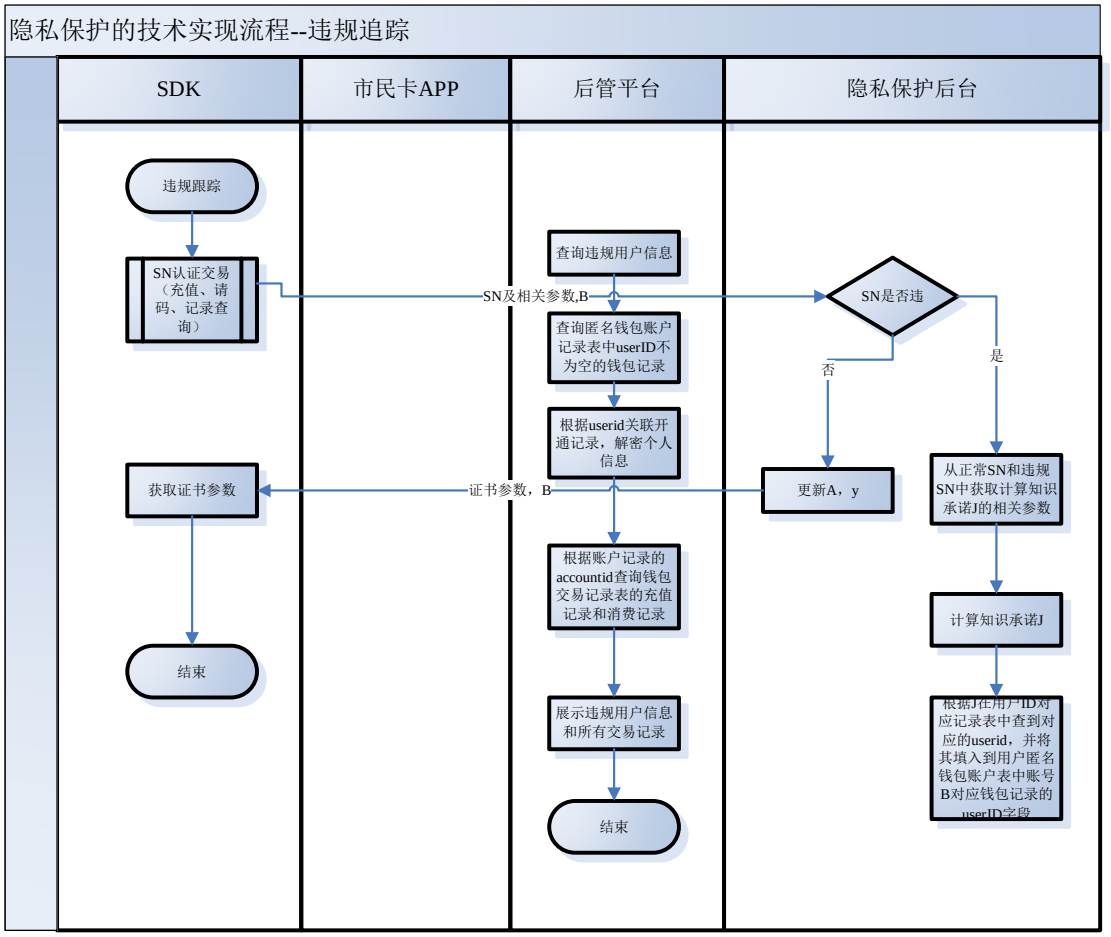

图 7：匿名码规追踪流程

2.8 匿名钱包余额返充

当客户端选择基于钱包交易不可追溯的匿名钱包方案时，用户每次充值均会生成不同的钱包账号 B 和后台账户编号 accountid，且不同钱包间不可链接，用户每次只能查询本次充值交易生成的钱包账号对应的交易记录（充值、扫码消费）。对于充值时存在未完成的扫码交易时，新钱包的充值将在一定时间后（如 7 天）才将原钱包的余返充到新充值交易生

成的匿名钱包账户中。因此需要通过定时任务完成旧钱包余额的返充，返充交易的业务流程如图 8 所示：

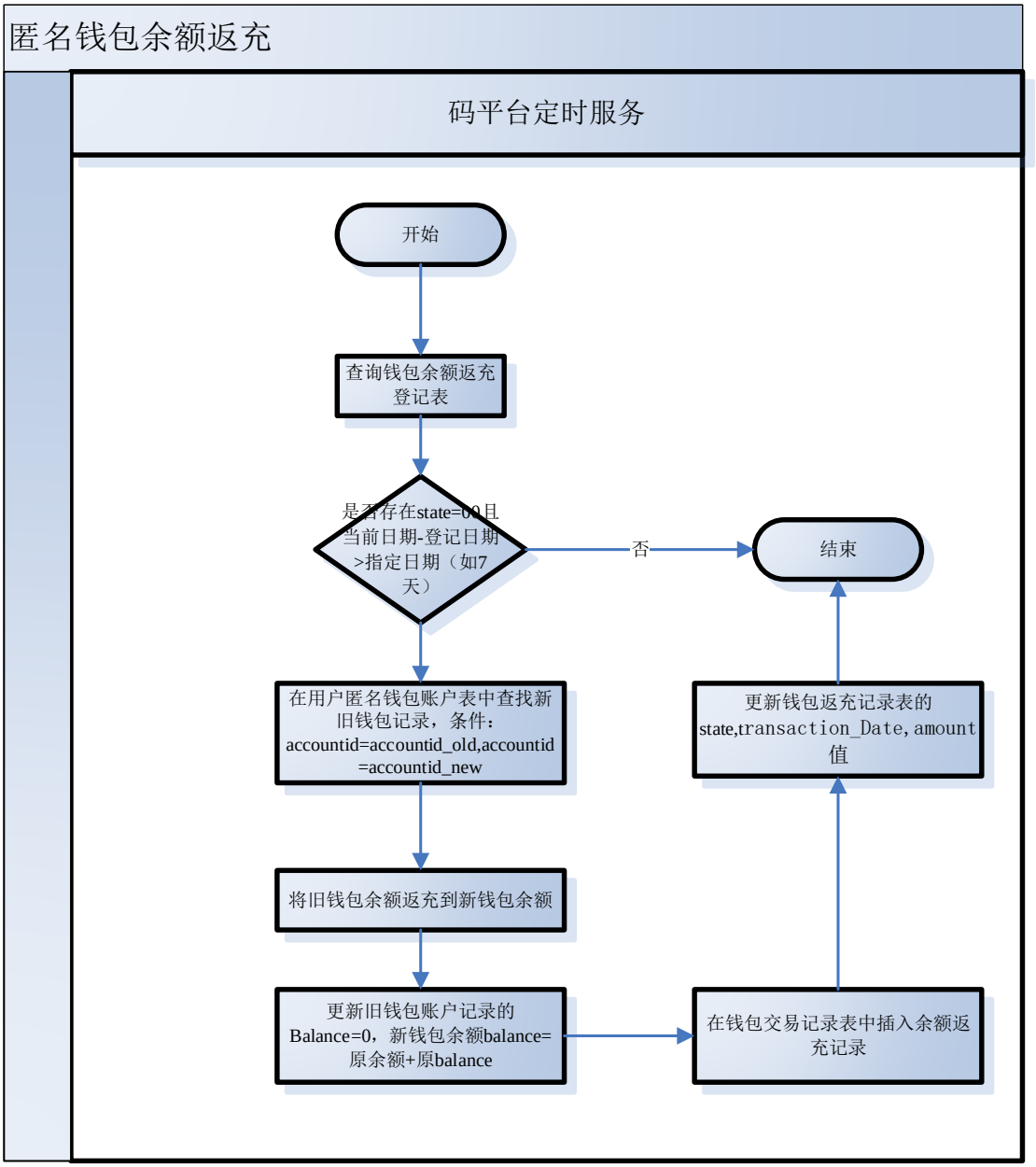

图 8：匿名码钱包返充流程

2.9 本地钱包数据备份

为满足用户更换手机导致账户信息变更以及钱包载体变更的要求，匿名码本地钱包需要具备可迁移性，因而需要具备钱包备份和恢复的功能。在 APP 端发起钱包备份请求时，首先隐私保护 SDK 向隐私保护后台发起钱包合法性验证，在满足合法性要求后，将本地的钱包信息以及用户的手机号上传至隐私保护后台保存，后期将根据用户的手机号查询钱包

备份信息并提供恢复服务，本地钱包在完成备份操作后，需要将本地的钱包状态置为不可用，避免前后端钱包信息的不一致性。具体流程见图 9。

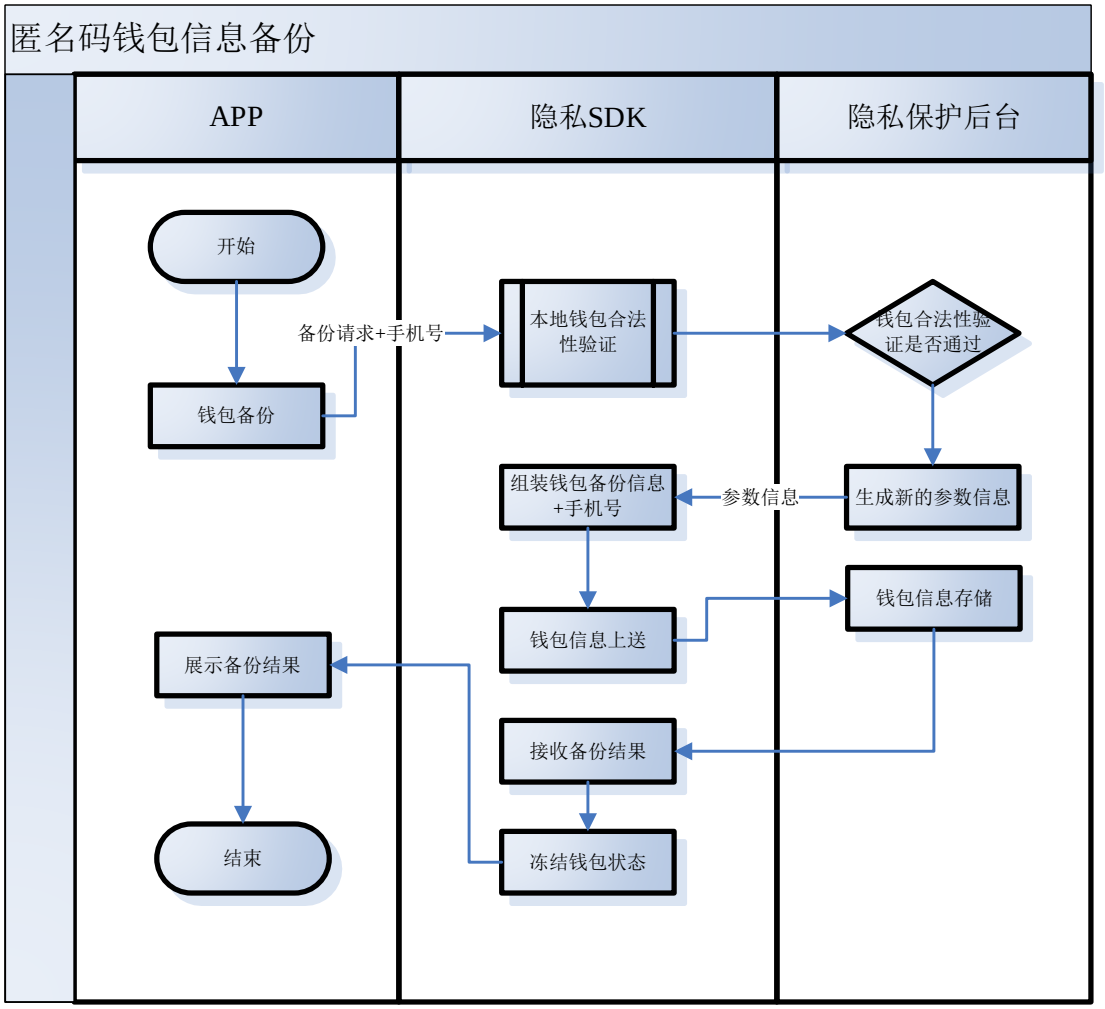

图 9：匿名码钱包备份流程

2.10 本地钱包数据恢复

在完成钱包数据的备份后，当需要将钱包数据迁移到新的移动载体后，可以通过 APP 端的钱包恢复功能从隐私保护后台将钱包数据恢复到隐私保护 SDK 中，数据恢复后，后台保存的钱包数据将失效，后续需要重新发起钱包备份交易，隐私保护后台将保存最新的备份数据。具体流程见图 10.

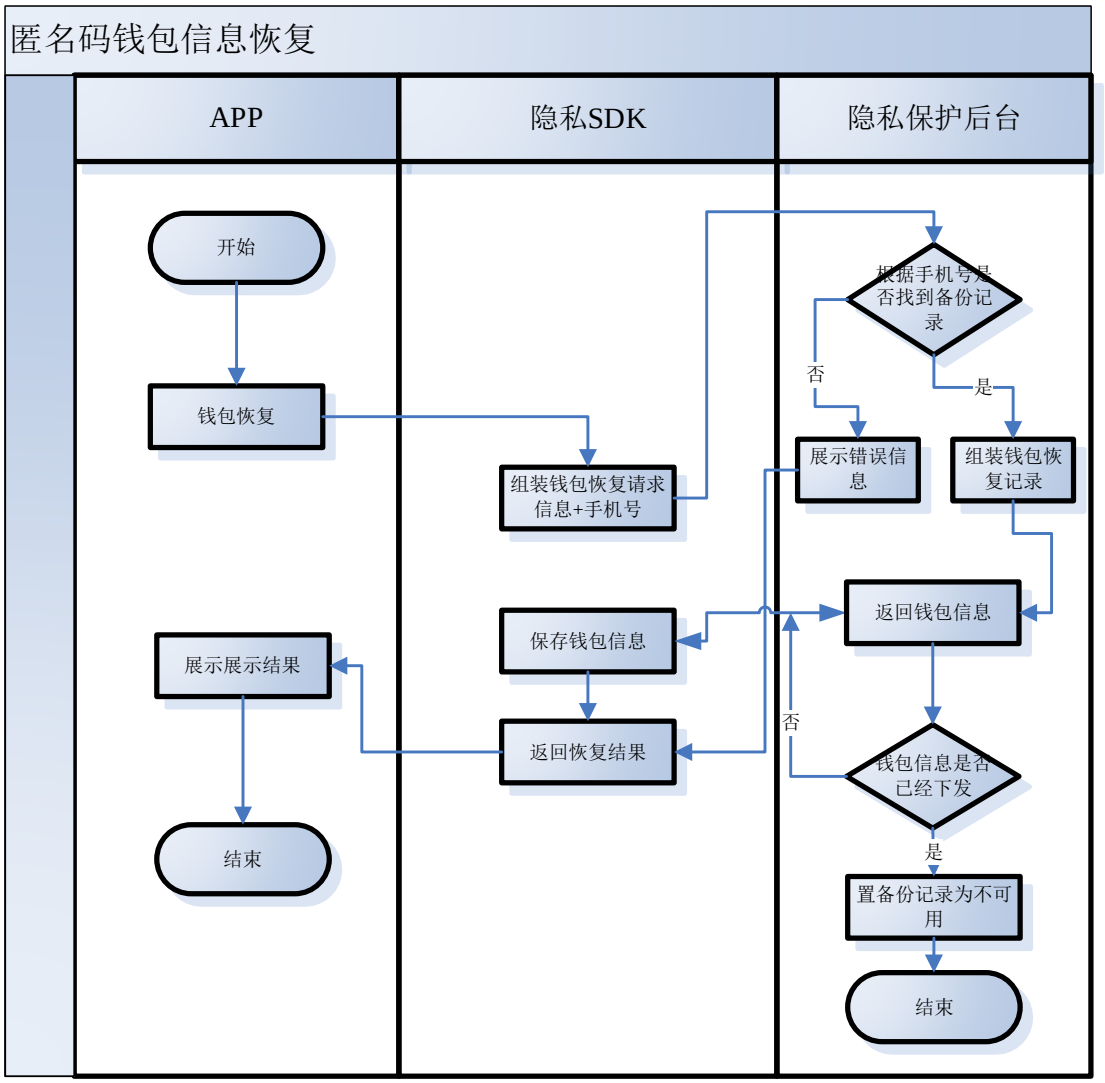

图 10：匿名码钱包恢复流程

2.11 匿名钱包余额退款

匿名钱包用户可以对匿名钱包发起退款操作，退款的金额应小于等于钱包余 额，客户填写退款的账号、个人信息（姓名、身份证号），客户端向匿名 SDK 发起验证申请，SDK 在验证本地钱包的合法性后，通过隐私保护后台验证退款的个人信息与注册的个人 信息是否相符并返回验证结果，在完成个人信息核验后，APP 客户端向服务端发起退款申 请，服务端收到后保存退款记录并向二维码平台发起退款申请，码平台在完成账户合法性 、未支付订单，退款金额等判断后，完成匿名账户记录表的余额更新 、退款记录保存等操 作，具体见图 11.

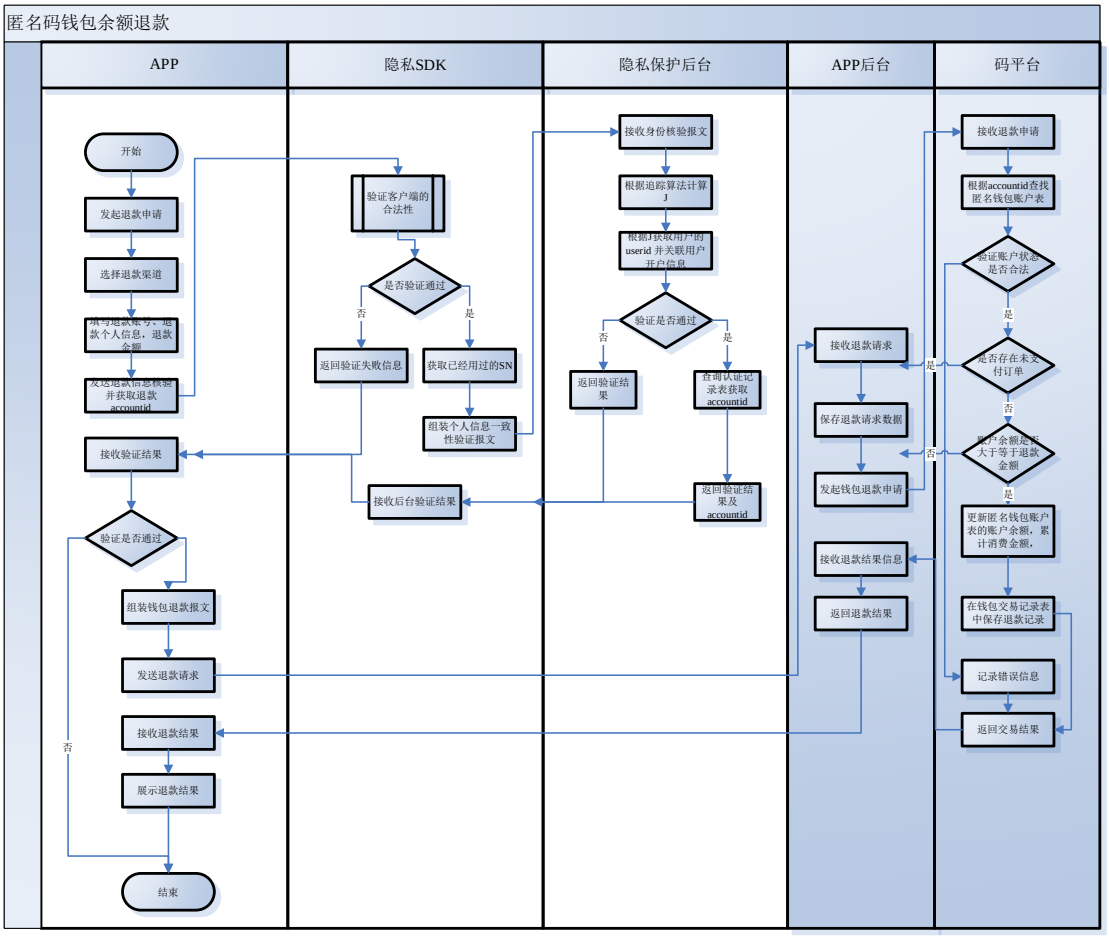

图 11：匿名码钱包退款流程

2.12 匿名钱包关闭

在用户不再需要使用匿名钱包后，可以发起匿名账户钱包的关闭操作，首先 APP 向隐私 SDK 发起合法性验证并获取 accountid，在完成核验后ＡＰＰ客户端向服务端发起关闭申请，ＡＰＰ服务端判断是否存在开通记录，如果存在则直接向二维码平台发起匿 名钱包关闭申请，码平台完成账户合法性，钱包余额等判断后，将匿名账户钱包置为关闭状态，同时保存关闭记录并向ＡＰＰ服务端返回关闭结果，ＡＰＰ服务端收到应答后，更新匿名码开通记录状态为关闭并返回结果给ＡＰＰ客户端，具体结果见图 12。

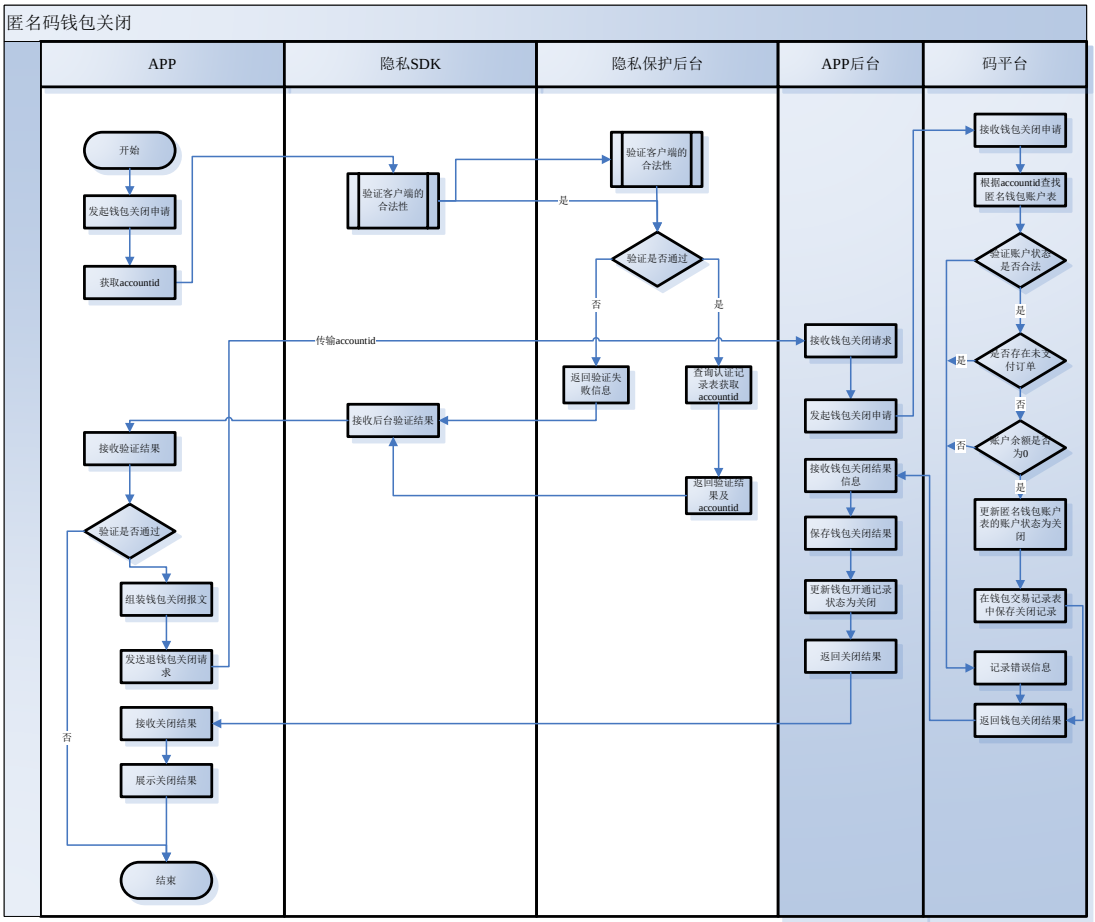

图 12：匿名码钱包关闭流程

三、数据库设计

匿名码的数据与码平台采用统一数据库，不同 schema 的模式独立建表，根据匿名码数据与乘车码独立纯纯的要求，需要保存匿名码开通的个人信息（个人信息需要加密存储）、钱包信息、钱包充值消费等交易记录信息、用户 ID 对应信息等，具体表结构表 1—表 5 所示：

3.1 用户匿名钱包账户表（ANONYMOUS_WALLET_ACCOUNTS）

B	Total_RECHARGE_amount	Total__consume_amount	BALANCE	ACCOUNTID	CREATION_DATE	IS_LOCKED	IS_DEACTIVATED	User_id
CHAR(24)	NUMBER(*)	NUMBER(*)	NUMBER(*)	Char(19)	DATE	CHAR(1)	CHAR(1)	Char(32)
匿名钱包账户	累计充值金额	累计消费金额	账户余额	账户ID，默认	钱包创建日期	异常情况的锁定	弃用（再次充值后新建一个	用户ID，账户

				云卡卡号			钱包账户，弃用上一个），0 正常，1：弃用	建立时为空，追踪异常行为时填写只是承诺对应的 user ID

3.2 用户 ID 对应记录表（USERID_RECORDS）

USER_ID	J	CREATION_DATE
CHAR(16)	CHAR(172)	DATE
用户知识承诺对应的 id	知识承诺	用户注册日期

3.3 认证交易记表 certification_TRANSACTIONS

SN	B	Certification_type	ACCOUNTID	USAGE_DATE	R	Is_used	C	State	Sequence
CHAR(172)	CHAR(24)	CHAR(2)	Char(19)	DATE	CHAR(172)	Char(1)	CHAR(24)	Char(2)	Char(16)
认证序列号	匿名钱包账户	认证类型，01：充值认证，02：请码认证；	账户 ID	认证日期	核心方案中的参数	是否使用，0：未使用，1：已使用（针对请码交易）	核心方案中的参数	认证记录状态；00：正常；01：重复使用；	请码序列号，默认全 0，当请码认证时填入 nm+14 位不重复序列号

3.3 钱包交易记录表（Wallet_Transactions）

paychannel	B	Pay_no	ACCOUNTID	Transaction_DATE	AMOUNT	Transaction_type	Account_type	Order_id	State
char（6))	CHAR(24)	varCHAR(30)	Char(19)	DATE	NUMBER(*)	CHAR(2)	Char(2)	Varchar(20)	Char(2)
资金来	匿名	充值支	账户	交易日期，	交易	交易类型	二维码	订单	订单

源；020001-银联，010002-支付宝，010001-微信	钱包账户	付订单号	ID,默认云卡卡号（钱包返交填充易写入钱包账号）	时间	金额	01：充值；02：消费；03:钱包余额返充 04：退款 05：关闭	账户类型；01：匿名码；	号，钱包返充交易填写旧钱包账号	状态；00：正常；0001：支付完成；02：充值完成；

3.4 匿名码开通信息表（anonymous_code_user_relationship）

bind_id	chnl_id	Open_id	Card_no	Card_type	biz_id	create_time	modi_time	state
Char(16)	Char(6)	Char(16)	Char(19)	Char(2)	Char(8)	date	date	Char(1)
绑定号	渠道号	存放accountId的MD5	卡号，存放accountId	码类型	APP平台编号	创建时间	最后修改时间	状态 0 正常 1 注销

3.5 钱包余额返充登记表（purse_Refund_record）

id	Register_date	accountid_old	accountid_new	Transaction_DATE	AMOUNT	Modify_DATE	State
char（8）	date	Char(19)	Char(19)	DATE	NUMBER	date	Char(2)
序号	登记日期，时间	旧账户ID	新账户ID	钱包余额返充日期，时间	返充金额	返充记录修改日期。时间	返充状态 00：未返充，01：已返充；

四、系统部署架构

基于码平台总体结构不变的原则，系统新建了隐私保护 SDK 和隐私保护后台，其中隐私保护后台与码平台同网段部署（或者同机部署），隐私保护 SDK 嵌入到市民卡 APP 当中，具体部署结构图如下所示：

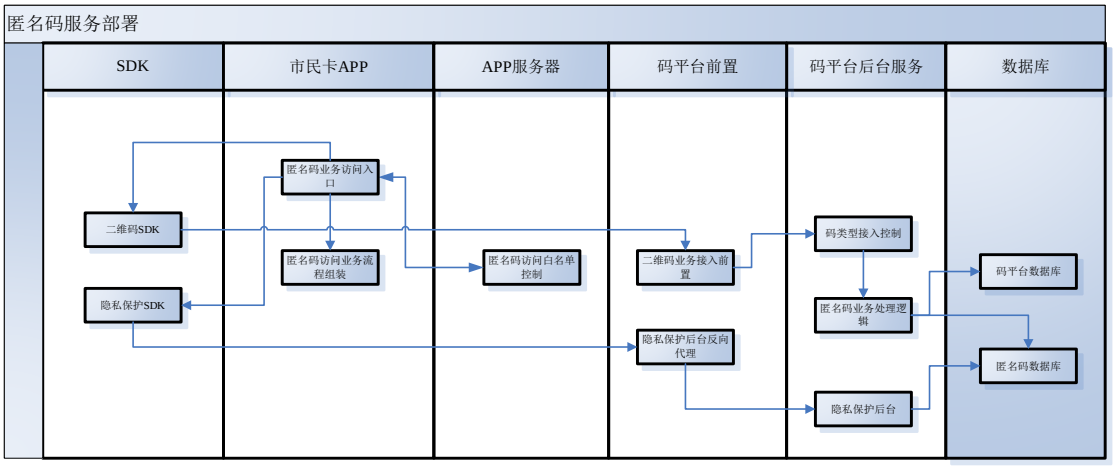

图 8：码平台改造服务部署结构

五、改造任务分工

六、改造时间安排